Editors’ Note

Managing Risk in an Information-Driven Digital World

Baker & McKenzie is pleased to provide you with access to this complimentary edition of our Global Privacy and Information Management Handbook which is now available for the first time in three user-friendly formats: via our Global Privacy App (free download from Apple Store or Google Play), online at http://globalprivacymatrix.bakermckenzie.com/ and, for our clients, in hardcopy. The new digital formats enable us to provide you with updated content in a more timely fashion as key developments unfold around the globe. You will now be able to access, in one place, Baker & McKenzie’s wide and growing range of privacy and information management resources.

Some noteworthy new and forthcoming features:

• coverage of 66 jurisdictions including new chapters for Croatia, Denmark, Finland, Greece, Iceland, Norway, New Zealand, Portugal, Uruguay, Paraguay, Saudi Arabia, California and Ukraine

• Global Privacy Matrix, an online tool that enables you to compare privacy and information management standards and requirements across jurisdictions

• iG360 - Information Governance Resource Center

• Data Security Knowledge Center

• BakerINFORM, a digital magazine focused on emerging global privacy and information management legal developments and trending topics

• Webinars, Whitepapers, and Business Intelligence

This new edition of the Handbook highlights the growing maturity of privacy laws around the globe and the convergence of such laws with an expanding range of information governance considerations, which are of top concern to global companies as more and more data are collected, used, and stored via various formats and for new business purposes. We are also witnessing a heightened awareness of data security risks and the impact of more robust breach notification requirements and regulatory enforcement. Finally, it is clear that technological and business innovation in areas such as connected cars, wearable devices, mobile payments, and digital marketing and user profiling is leading to new and more refined interpretations of existing laws and challenging data regulators to provide greater guidance to data controllers that deploy such technologies and pursue such activities.
Once again, we want to thank our friends at the International Association of Privacy Professionals (“IAPP”) for their help in making a special version of the Handbook available to IAPP members via our Global Privacy App. Baker & McKenzie is proud to be a lead supporter of the IAPP and of the fact that we have more IAPP Certified Information Privacy Professionals than any other legal service provider in the world.

Theo Ling
Chair, Baker & McKenzie Global Privacy & Information Management Leadership Team
Baker & McKenzie’s Global Privacy Leadership Team

**Anne-Marie Allgrove (Sydney)**
+61 2 8922 5274  
anne-marie.allgrove@bakermckenzie.com

**Guillermo Cervio (Buenos Aires)**
+54 11 4310 2223  
guillermo.cervio@bakermckenzie.com

**Ken Chia (Singapore)**
+65 6434 2558  
ken.chia@bakermckenzie.com

**Lothar Determann (Palo Alto)**
+1 650 856 5533  
lothar.determann@bakermckenzie.com

**Francesca Gaudino (Milan)**
+39 02 76231 452  
francesca.gaudino@bakermckenzie.com

**Brian Hengesbaugh (Chicago)**
+1 312 861 3077  
brian.hengesbaugh@bakermckenzie.com

**Theo Ling (Toronto)**
+1 416 865 6954  
theo.ling@bakermckenzie.com

**Carolina Pardo (Bogota)**
+57 1 634 1559  
carolina.pardo@bakermckenzie.com

**Michael Schmidl (Munich)**
+49 89 5 52 38 155  
michael.schmidl@bakermckenzie.com

**Harry Small (London)**
+44 20 7919 1914  
harry.small@bakermckenzie.com

**Ken Takase (Tokyo)**
+81 3 6271 9752  
kensaku.takase@bakermckenzie.com
Associate Editor

Joan Melcar T. Tan (Manila)
+632 558 9421
joanmelcar.tan@bakermckenzie.com
Contributing Lawyers

Argentina
Guillermo Cervio
Buenos Aires
Tel: +54 11 4310 2223
guillermo.cervio@bakermckenzie.com

Roberto Grané
Buenos Aires
Tel: +54 11 4310 2214
roberto.grane@bakermckenzie.com

Argentina
Anne-Marie Allgrove
Sydney
Tel: +61 2 8922 5274
anne-marie.allgrove@bakermckenzie.com

Australia
Patrick Fair
Sydney
Tel: +61 2 8922 5534
patrick.fair@bakermckenzie.com

Adrian Lawrence
Sydney
Tel: +61 2 8922 5204
adrian.lawrence@bakermckenzie.com

Toby Patten
Melbourne
Tel: +61 3 9617 4456
toby.patten@bakermckenzie.com

Austria
Lukas Feiler
Vienna
Tel: +43 1 24250 450
lukas.feiler@bakermckenzie.com

Azerbaijan
Gunduz Karimov
Baku
Tel: +994 12 4971 801
gunduz.karimov@bakermckenzie.com

Jamil Alizada
Baku
Tel: +994 12 4971 801
jamil.alizada@bakermckenzie.com

Belgium
Elisabeth Dehareng
Brussels
Tel: +32 2 639 36 11
elisabeth.dehareng@bakermckenzie.com

Daniel Fesler
Brussels
Tel: +32 2 639 36 11
daniel.fesler@bakermckenzie.com

Brazil
Esther Flesch
Sao Paulo
Tel: +55 11 3048 6940
esther.flesch@bakermckenzie.com

Bruno Maeda
Sao Paulo
Tel: +55 11 3048 6838
bruno.maeda@bakermckenzie.com

Flavia Rebello
Sao Paulo
Tel: +55 11 3048 6851
flavia.rebello@bakermckenzie.com

Canada
Lisa Douglas
Toronto
Tel: +416 865 6972
lisa.douglas@bakermckenzie.com

Arlan Gates
Toronto
Tel: +416 865 6978
arlan.gates@bakermckenzie.com
Kazakhstan

Gulnur Bekmukhanbetova
Almaty
Tel: +7 727 330 0500
Tel: +7 727 250 99 45
gulnur.bekmukhanbetova
@bakermckenzie.com

Azamat Kuatbekov
Almaty
Tel: +7 727 330 0500
Tel: +7 727 250 99 45
azamat.kuatbekov@bakermckenzie.com

Luxembourg

Audrey Rustichelli
Luxembourg
Tel: +352 261844 249
audrey.rustichelli@bakermckenzie.com

Malaysia

Woo Wei Kwang
Kuala Lumpur
Tel: +603 2298 7898
weikwang.woo@wongpartners.com

Ken Boon Low
Kuala Lumpur
Tel: +603 2298 7988
kenboon.low@wongpartners.com

Shameen Mohd. Haaziq Pillay
Kuala Lumpur
Tel: +603 2298 7943
shameen.mohd.haaziqpillay
@wongpartners.com

Mexico

Sergio Legorreta-Gonzalez
Mexico City
Tel: +52 55 5279 2954
sergio.legorreta-gonzalez
@bakermckenzie.com

Carlos Vela-Trevino
Mexico City
Tel: +52 55 5279 2911
carlos.vela-trevino@bakermckenzie.com

Netherlands

Remke Scheepstra
Amsterdam
Tel: +31 20 5517 831
remke.scheepstra@bakermckenzie.com

Wouter Seinen
Amsterdam
Tel: +31 20 5517 161
wouter.seinen@bakermckenzie.com

New Zealand

Karen Ngan
Auckland
Tel: +64 9 977 5080
karen.ngan@simpsongrierson.com

Carl Blake
Auckland
Tel: +64 9 977 5163
carl.blake@simpsongrierson.com

Norway

Espen Sandvik
Oslo
Tel: +47 98 29 45 41
esa@adeb.no

Paraguay

Nestor Loizaga
Asuncion
Tel: 595 21 318 3000 ext. 117
nloizaga@ferrere.com

Peru

Javier Tovar
Lima
Tel: +51 1 618 8500 Ext. 550
javier.tovar@bakermckenzie.com

Teresa Tovar
Lima
Tel: +51 1 618 8500 Ext. 552
teresa.tovar@bakermckenzie.com

Viviana Chavez
Lima
Tel: +51 1 618 8500 Ext. 421
viviana.chavez@bakermckenzie.com
Philippines
Bienvenido Marquez
Manila
Tel: +63 2 819 4936
bienvenido.marquez
@quisumbingtorres.com

Divina Ilas-Panganiban
Manila
Tel: +63 2 819 4961
divina.llas-panganiban
@quisumbingtorres.com

Carlo Abarquez
Manila
Tel: +63 2 819 4993
carlo.abarquez
@quisumbingtorres.com

Poland
Magdalena Kogut-Czarkowska
Warsaw
Tel: +48 22 445 3452
magdalena.kogut-czarkowska
@bakermckenzie.com

Radoslaw Nożykowski
Warsaw
Tel: +48 22 445 3210
radoslaw.nozykowski
@bakermckenzie.com

Jakub Falkowski
Warsaw
Tel: +48 22 445 3294
jakub.falkowski@bakermckenzie.com

Russia
Edward Bekeschenko
Moscow
Tel: +7 495 787 2700
edward.bekeschenko
@bakermckenzie.com

Ekaterina Kobrin
Moscow
Tel: +7 495 787 2700
ekaterina.kobrin@bakermckenzie.com

Evgeny Reyzman
Moscow
Tel: +7 495 787 2700
evgeny.reyzman@bakermckenzie.com

Dmitry Lysenko
Moscow
Tel: +7 495 787 2700
dmitry.lysenko@bakermckenzie.com

Saudi Arabia
George Sayen
Riyadh
Tel: + 966 11 265 8900, Ext. 8911
george.sayen@bakermckenzie.com

Aisha Gondal
Riyadh
Tel: + 966 11 265 8900, Ext. 8913
aisha.gondal@bakermckenzie.com

Haifa Bahaian
Riyadh
Tel: + 966 11 265 8900, Ext. 8968
haifa.bahaian@bakermckenzie.com

Judes Abboud
Dubai
Tel: + 971 442 30080
judes.abboud@bakermckenzie.com

Baker & McKenzie
Singapore

Ken Chia
Singapore
Tel: +65 6434 2558
ken.chia@bakermckenzie.com

Quan Nguyen
Singapore
Tel: +65 6434 2592
quan.nguyen@bakermckenzie.com

South Africa

Darryl Bernstein
Johannesburg
Tel: +27 (0) 11 911 4367
Darryl.bernstein@bakermckenzie.com

Widaad Ebrahim
Johannesburg
Tel: +27 (0) 11 911 4384
widaad.ebrahim@bakermckenzie.com

Deepa Ramjee
Johannesburg
Tel: +27 (0) 11 911 4368
deepa.ramjee@bakermckenzie.com

South Korea

Boseong Kim
Seoul
Tel: +82 2 721 4130
boskim@kcllaw.com

Junghwa Lee
Seoul
Tel: +82 2 721 4147
jhlee@kcllaw.com

Spain

Raul Rubio
Madrid
Tel: +34 91 436 6639
raul.rubio@bakermckenzie.com

Jordi Masdevall
Barcelona
Tel: +34 93 206 0820
jordi.masdevall@bakermckenzie.com

Maria Pons
Barcelona
Tel: +34 932551117
maria.pons@bakermckenzie.com

Rosario Alvarez
Madrid
Tel: +34 91 230 4513
rosario.alvarez@bakermckenzie.com

Sweden

Sten Bauer
Stockholm
Tel: +46 8 566 177 16
sten.bauer@bakermckenzie.com

Johan Strand
Stockholm
Tel: +46 8 566 177 41
johan.strand@bakermckenzie.com

Switzerland

Nicolas Passadelis
Zurich
Tel: +41 44 384 1209
nicolas.passadelis@bakermckenzie.com

Taiwan

H. Henry Chang
Taipei
Tel: +886 2 2715 7259
henry.chang@bakermckenzie.com

Chris Tsai
Taipei
Tel: +886 2 2715 7310
chris.tsai@bakermckenzie.com

Thailand

Dhiraphol Suwanprateep
Bangkok
Tel: +66 02 636 2000 Ext. 4950
dhiraphol.suwanprateep@bakermckenzie.com
Pattaraphan Paiboon  
Bangkok  
Tel: +66 02 636 2000 Ext. 4568  
pattaraphan.paiboon@bakermckenzie.com

Turkey  
Hakki Can Yildiz  
Istanbul  
Tel: +90 212 376 64 54  
can.yildiz@bakermckenzie.com

Can Sozer  
Istanbul  
Tel: +90 212 376 64 43  
can.sozer@bakermckenzie.com

Ukraine  
Oleksiy Stolyarenko  
Kyiv  
Tel: + 380 44 590 0101  
oleksiy.stolyarenko@bakermckenzie.com

United Kingdom  
Robbie Downing  
London  
Tel: +44 20 7919 1161  
robbie.downing@bakermckenzie.com

Benjamin Slinn  
London  
Tel: +44 20 7919 1783  
benjamin.slinn@bakermckenzie.com

United States  
Amy de La Lama  
Chicago  
Tel: +1 312 861 2923  
amy.delalama@bakermckenzie.com

Lothar Determann  
Palo Alto  
Tel: +1 650 856 5533  
lothar.determann@bakermckenzie.com

Brian Hengesbaugh  
Chicago  
Tel: +1 312 861 3077  
brian.hengesbaugh@bakermckenzie.com

Michael Stoker  
Chicago  
Tel: +1 312 861 2870  
michael.stoker@bakermckenzie.com

Heather Mantegna  
Chicago  
Tel: +1 312 861 8808  
heather.mantegna@bakermckenzie.com

Karen Sewell  
Chicago  
Tel: +1 312 861 8228  
karen.sewell@bakermckenzie.com

Lindsay Martin  
Chicago  
Tel: +1 312 861 2949  
lindsay.martin@bakermckenzie.com

Brandon Moseberry  
Chicago  
Tel: +1 312 861 8265  
brandon.moseberry@bakermckenzie.com

Marc Elzweig  
San Francisco  
Tel: +1 415 576 3018  
marc.elzweig@bakermckenzie.com

Michael Egan  
Washington, D.C.  
Tel: +1 202 452 7022  
michael.egan@bakermckenzie.com

Uruguay  
Martin Pesce  
Montevideo  
Tel: +598 2900 1000 ext. 1200  
mpesce@ferrere.com

Stephanie Bresque  
Montevideo  
Tel: +598 2900 1000 ext. 1531  
sbresque@ferrere.com
Venezuela

**Maria Eugenia Salazar**
Caracas
Tel: +58 212 276 5161
mariaeugenia.salazar
@bakermckenzie.com

**Luis Miguel Vicentini**
Caracas
Tel: +58 212 276 5069
luis.miguel.vicentini@bakermckenzie.com

Vietnam

**Andrew Fitanides**
Ho Chi Minh City
Tel: +84 8 3520 2687
andrew.fitanides@bakermckenzie.com

**Tran Manh Hung**
Hanoi
Tel: +84 4 3936 9398
tmh@bmvn.com.vn

**Minh Tri Quach**
Hanoi
Tel: +84 4 3936 9605
minhtri.quach@bmvn.com.vn

**Yee Chung Seck**
Ho Chi Minh City
Tel: +84 8 829 6234
yeechung.seck@bakermckenzie.com

*This list includes just some of our global Privacy practitioners. To find a Baker & McKenzie lawyer or other professional, please visit www.bakermckenzie.com.*
# Table of Contents

Editors' Note.................................................................................................................. i  
Contributing Lawyers.................................................................................................... v  
Argentina ....................................................................................................................... 1  
Australia ...................................................................................................................... 15  
Austria ........................................................................................................................... 27  
Azerbaijan .................................................................................................................... 37  
Belgium .......................................................................................................................... 43  
Brazil ............................................................................................................................. 61  
Canada .......................................................................................................................... 73  
Alberta, Canada .......................................................................................................... 89  
British Columbia, Canada .......................................................................................... 100  
Manitoba, Canada ........................................................................................................ 110  
Ontario, Canada .......................................................................................................... 120  
Quebec, Canada .......................................................................................................... 129  
Chile ............................................................................................................................ 137  
China ............................................................................................................................ 143  
Colombia ...................................................................................................................... 155  
Croatia .......................................................................................................................... 171  
Czech Republic ......................................................................................................... 185  
Denmark ....................................................................................................................... 197  
Egypt ............................................................................................................................. 215  
Finland .......................................................................................................................... 223  
France ........................................................................................................................... 239  
Germany ....................................................................................................................... 257  
Greece ........................................................................................................................... 271  
Hong Kong .................................................................................................................. 291  
Hungary ........................................................................................................................ 311  
Iceland .......................................................................................................................... 327  
India .............................................................................................................................. 343
<table>
<thead>
<tr>
<th>Country</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indonesia</td>
<td>355</td>
</tr>
<tr>
<td>Ireland</td>
<td>363</td>
</tr>
<tr>
<td>Israel</td>
<td>377</td>
</tr>
<tr>
<td>Italy</td>
<td>395</td>
</tr>
<tr>
<td>Japan</td>
<td>409</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>421</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>431</td>
</tr>
<tr>
<td>Malaysia</td>
<td>443</td>
</tr>
<tr>
<td>Mexico</td>
<td>453</td>
</tr>
<tr>
<td>Netherlands</td>
<td>461</td>
</tr>
<tr>
<td>New Zealand</td>
<td>473</td>
</tr>
<tr>
<td>Norway</td>
<td>485</td>
</tr>
<tr>
<td>Paraguay</td>
<td>497</td>
</tr>
<tr>
<td>Peru</td>
<td>505</td>
</tr>
<tr>
<td>Philippines</td>
<td>513</td>
</tr>
<tr>
<td>Poland</td>
<td>525</td>
</tr>
<tr>
<td>Portugal</td>
<td>537</td>
</tr>
<tr>
<td>Russia</td>
<td>561</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>571</td>
</tr>
<tr>
<td>Singapore</td>
<td>581</td>
</tr>
<tr>
<td>South Africa</td>
<td>593</td>
</tr>
<tr>
<td>South Korea</td>
<td>607</td>
</tr>
<tr>
<td>Spain</td>
<td>617</td>
</tr>
<tr>
<td>Sweden</td>
<td>631</td>
</tr>
<tr>
<td>Switzerland</td>
<td>643</td>
</tr>
<tr>
<td>Taiwan</td>
<td>653</td>
</tr>
<tr>
<td>Thailand</td>
<td>663</td>
</tr>
<tr>
<td>Turkey</td>
<td>675</td>
</tr>
<tr>
<td>Ukraine</td>
<td>687</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>697</td>
</tr>
<tr>
<td>United States</td>
<td>711</td>
</tr>
</tbody>
</table>
United States California Privacy Laws .......................... 717
United States Children’s Online Privacy Protection Act (“COPPA”) .... 724
United States Gramm-Leach-Bliley Act and Fair Credit Reporting Act ...... 732
United States Health Insurance Portability and Accountability Act ........ 743
United States State Data Security Laws ........................................ 757
United States State Security Breach Notification Laws ................... 763
Uruguay ....................................................................................... 769
Venezuela ..................................................................................... 783
Vietnam ......................................................................................... 789
Baker & McKenzie Offices Worldwide ........................................ 799
Argentina

Guillermo Cervio
Buenos Aires
Tel: +54 11 4310 2223
guillermo.cervio@bakermckenzie.com

Roberto Grané
Buenos Aires
Tel: +54 11 4310 2214
roberto.grane@bakermckenzie.com
1. Recent Privacy Developments

First ruling from the National Supreme Court of Justice limiting the liability of search engines

On 28 October 2014, the National Supreme Court of Justice ruled in favor of search engines in the case filed by an Argentine model who claimed that her privacy, honor, and intellectual property rights were violated, after she found that search results linked her name to sites with manipulated sexual content. The Supreme Court ruled that the liability of search engines is based on the “negligence system” (as opposed to the “strict liability” system), whereby search engines will only be liable if, after receiving notice of the existence of illicit content, they do not proceed to remove the same. As this is the first judgment issued by the National Supreme Court with respect to the liability of search engines, this will prove to be a significant case which will affect cases with similar factual backgrounds.

New telecom law: Argentina Digital and Net Neutrality obligations

On 16 December 2014, the National Congress enacted the Argentina Digital Law No. 27,078, which regulates information technology and communication services (“IT/C Services”), declaring them as public services and creating a series of obligations applicable to IT/C service providers.

The Argentina Digital law also regulates Net Neutrality, forbidding IT/C service providers from blocking, interfering, discriminating, degrading or restricting the use, delivery, reception or access to any content, application, service or protocol, unless there is a judicial order in place or express request from the user. The law also prohibits IT/C service providers from calculating prices for Internet access with regard to the content, services, protocols or applications included in the service plan.

Amendment and restatement of the National Civil and Commercial Codes

On 8 October 2014, the National Congress resolved to issue an amendment and restatement of the Civil and Commercial Code, to be effective on 1 August 2015. As a result, several civil and commercial provisions have been amended, and new rules have been inserted. For instance, from an e-commerce perspective, the new Civil and Commercial Code provides that any contractual disputes arising from electronic contracts will be resolved by the authorities of the jurisdiction in which the consumer has received or should have received the product or service; any clause providing otherwise will be considered null and void.

New National “Do Not Call” List

On 2 July 2014, the Argentine Congress enacted Law No. 26,951 which creates a “Do Not Call” list applicable at a national level. The purpose of the law is to protect consumers against abusive telemarketing activities designed
to promote or sell unrequested products or services. Any natural or legal person has the right to register their mobile or fixed phone numbers with such list for free. Those who promote products or services through telemarketing activities are prohibited from contacting any number registered on the list, and are required to search the registry at least once every 30 (thirty) days and update their internal call list accordingly.

Companies that have a pre-existing relationship with a consumer are exempted from such restriction, provided that the calls specifically relate to the purpose of the agreement with the consumer and are performed in a reasonable manner and within business hours. Electoral campaigns or campaigns destined for public welfare, health emergency or security emergency are also excluded from such restriction. The supervisory authority is the Argentine Personal Data Protection Authority.

On 17 December 2014, the Executive Branch issued Decree No. 2501/2014, which regulates the procedural aspects of the registration and the manner of reporting infringements.

**New withholding regime for the City of Buenos Aires for audiovisual entertainment rendered through the Internet**

On 3 September 2014, the Official Gazette of the City of Buenos Aires published Resolution N° 593/AGIP/14, which establishes a withholding tax regime on gross revenue for online subscriptions of movies, TV and other audiovisual entertainment (e.g., movies and series) that are rendered through the Internet to TVs, computers and other Internet-connected devices, as well as subscription to buy and/or rent digital content related to music, games, videos, etc. The resolution designates the issuers of credit, debit and purchase cards involved in the detailed operations as withholding agents on the payments made to the companies that provide those services. The withholding rate is 3% on the net price of the transaction.

**New procedural regulation for Digital Signature Certifiers applications**

The Digital Signature Law No. 25,506 enumerates the legal grounds for the issuance and use of digital signature certificates in Argentina. In Argentina, electronic signatures are not at the same level of enforceability as written and/or digital signatures. According to the law, instruments signed with digital signatures are presumed to be signed by the signatory registered with the certifying licensee and, in the case that a party denies the authenticity of the digital signature, such party must provide evidence to bolster their position. On the contrary, instruments signed with electronic signatures do not have this legal presumption. If a party denies the authenticity of an electronic signature, the enforcing party must prove its authenticity to the Courts.

The Digital Signature Law further establishes that companies that wish to operate as Certifying Authorities must obtain an operating license with the National Authority.
On 30 October 2014, the Chief Head of Ministries enacted the Administrative Decision No. 927/14, which establishes the procedural rules and requirements applicable to the application process for obtaining an operation license with the National Authority.

**App Privacy Guidelines**

On 10 April 2015, the Argentine National Data Protection Authority issued Disposition No. 18/2015 which creates “Best Practice Guidelines for the Development of Apps”. This guidance is targeted at app developers: it focuses on the design and development of apps and the need to keep privacy top of mind in that creative process. The guidelines cover new concepts such as “Privacy by Default” and “Privacy by Design” and describe different security measures that can be used by app developers to protect the personal data of users in accordance with Argentine privacy laws and regulations.

**New regulations on the use of drones**

From a regulatory perspective, on 15 July 2015, the National Civil Aviation Administration (“ANAC”) enacted Resolution No. 527/2015 (the “Resolution”). The Resolution sets forth the requirements and conditions for the use and operation of unmanned aerial vehicles, or “UAVs” (commonly referred to as “Drones”). The requirements include, among others, limitations on the use of Drones within certain areas and/or heights, obligation to maintain permanent visual contact with the Drone, and registration of the Drone under the corresponding registry. In addition, owners of Drones will need to obtain a psycho-physiological certificate and an insurance for damages caused by the Drone. The Regulation also classified Drones into the following three categories: (i) small Drones (up to 10 kg); (ii) intermediary Drones (between 10 kg and 150 kg); and (iii) big Drones (over 150 kg). Certain exceptions are contemplated for the use of small Drones for recreational purposes. The Resolution will come into force on 12 November 2015.

From a privacy perspective, on 27 May 2015, the National Data Protection Authority issued Disposition No. 20/2015 (the “Disposition”). The Disposition approves the “Legal Terms for the Collection of Personal Data through Drones or UAVs” and the “Privacy Recommendations for the use of Drones or UAVs”. The Disposition covers any personal data collection activities performed using photographic, film, audio or any other kind of material, stored in digital format, made by unmanned aerial vehicles (UAVs) or drones, for recording purposes or any other treatment. The Disposition also provides rules for drones or UAVs used for scientific or recreational purposes. The Disposition became effective on 4 June 2015.

2. **Emerging Privacy Issues and Trends**

**Mandatory Breach Notification.** There is no requirement to report a breach of the security of personal data. However, best practices would indicate that it is necessary to alert the data owners about the breach in certain cases. It is
likely that the Argentine Data Protection Authority will closely monitor the data controller’s and data processor’s adoption of security measures and registration of databases.

**Online Direct Marketing.** There are no restrictions regarding online direct marketing. Nevertheless, when engaging in direct marketing using various electronic channels, companies should ensure that consumers are given the freedom to choose whether or not to engage in a relationship or receive communications from companies.

**Anti-spam Legislation.** There is no specific anti-spam legislation in Argentina. The unsolicited commercial electronic messages should contain the procedure by which consumers can avoid receiving unsolicited product or service information. In addition, this information should also be supported with articles from the Data Protection Law and its Executive Order.

**Bring Your Own Device.** The two main concerns regarding this matter are the following: (i) Monitoring activities. Usually, the employer informs its employees that by enrolling in the so called “Mobile Device Policy”, they allow their devices to be remotely monitored. As a general rule, an employer may not monitor an employee’s personal e-mails unless there is a genuine suspicion of the employee being disloyal, acting in breach of company policies or that the company has a serious concern that the employee is using the IT equipment for (for example) pornographic or racist purposes (nevertheless, as per current trends, even in these cases, consent of the Data Owner may be required. This matter is highly debatable); and (ii) Personal information. It is likely that in case of termination of the labor contract with cause, the employee alleges that the loss of certain information will cause damage. The company should refrain from maintaining information that could be clearly considered as private information of the employees.

**Social Media.** The main impact of social media is in connection with its use by employees. It is advisable that employers put into effect policies regarding the proper use of social media sites. Employees who are allowed to access social media sites during working hours should do so reasonably and must act in good faith. The employer may prohibit or limit the time spent on these sites, and sanction any infringement thereof. Sanctions should be fair and reasonable.

**Employee Monitoring.** Monitoring of employees’ computers is a sensitive matter. Employers should have in place an internal policy -dually notified to employees—which clearly states that computers, emails received and sent from the company’s email addresses, and other IT resources used or provided by the company are work tools and therefore belong to the company, that said resources should not be used by employees for personal purposes, and that at any time the company may monitor the activities of the employees while using the work tools/resources provided by the company. It is advisable that
the internal policy clearly state, in highlighted fashion, that employees have no expectation of privacy over work tools.

**Documents and Records Retention Policy.** Documents and records retention policies apply, with different criteria depending on the content of the corresponding documents. For example, under the Argentine Civil and Commercial Code, companies have the duty to keep their corporate and accounting books for ten (10) years. Also, the statute of limitations for the enforcement of most civil and commercial actions is ten (10) years. In this regard, a ten (10) year retention period policy would be appropriate for commercial related documents, unless there is a special legal obligation to retain certain documents for a longer period of time. Different statutes of limitation apply for other areas (2 years for labor matters, 10 years for social security matters and 5 years for tax matters.)

**Cookie Consent Requirement.** The use of cookies and web beacons would be, in principle, permitted provided that proper notice on their use is given to users (e.g., in the privacy policy). In this regard, the terms and conditions of the privacy policy should indicate that by accepting said terms and conditions, the users accept the deployment and use of cookies and web beacons. It is also recommended that the privacy policy describe the manner in which the cookies can be deactivated (i.e., from browsers) and the consequences for doing so.

**Do Not Call Registry.** On 2 July 2014, the Argentine Congress enacted Law No. 26,951 which creates a “Do Not Call” list applicable at a national level. Pursuant to this law, any natural or legal person has the right to register their mobile or fixed phone numbers with such list on a free basis. Those who promote products or services through telemarking activities are prohibited from contacting any number registered with the list, and are required to search the registry at least once every 30 (thirty) days and update their internal call list accordingly. Companies that have a pre-existing relationship with a consumer are exempted from such restriction, provided that the calls specifically relate to the purpose of the agreement with the consumer and are performed in reasonable manner and within business hours. Electoral campaigns or campaigns destined for public welfare, health emergency or security emergency are also excluded from such restriction. The supervisory authority is the Argentine Personal Data Protection Authority. On 17 December 2014 the Executive Branch issued the Decree No. 2501/2014, which regulates the procedural aspects of the registration and report of infringements.

**Click-Through/ Click-wrap/ Electronic Contracting.** There is no integrated regulation that specifically governs electronic contracting, and therefore the general rules for contracts apply. The Argentine Civil and Commercial Code recognizes the existence of electronic contracts, and requires the provider to provide consumers with all the necessary information to use the electronic
method in a correct manner and understand the risks from using the same. It further establishes that the applicable jurisdiction for electronic contracts is determined by the ‘place of performance’, which corresponds to the place in which the consumer received, or should have received, the goods or services. From a probationary perspective, consent can be validly expressed by tacit or express means, and therefore the contract so entered will be subject to evidence—in case it is challenged by one of the parties to the contract. According to limited legal precedents, local courts would consider: (i) the evidence regarding identities of the parties, and acceptance of the agreement by electronic means; (ii) if the content of the electronic contract has (or has not) been altered once it has been accepted; and (iii) if the messages exchanged between the parties have actually been sent and received by said parties (e.g., acknowledgement receipt, confirmatory e-mails, etc.)

Electronic Signature. In Argentina, electronic signatures are not at the same level of enforceability as written and/or digital signatures. According to the Digital Signatures Law No. 25,506, instruments signed with digital signatures are presumed to be signed by the signatory registered with the certifying licensee and, in the case a party denies the authorship of the digital signature, then such party must evidence their position. On the contrary, instruments signed with electronic signatures do not have this legal presumption; if a party denies the authorship of an electronic signature, then the enforcing party must prove such authorship to the Courts.

Binding Corporate Rules. The Argentine Data Protection Authority has not approved the Binding Corporate Rules or “Burrs”, understood as those rules developed for intra-organizational transfers of personal data across borders.

Data Protection Enforcement. The Argentine Data Protection Authority is active in enforcing applicable regulations. However, such approach would be friendly and business-oriented in the sense that usually, before applying fines or other penalties, the Argentine Data Protection Authority would seek compliance or corrective actions from the erring companies.

Cybercrime/ Cybersecurity. As already indicated, in case of data breach for cybercrimes, there is no need to report to the Argentine Data Protection Authority, but it is highly recommended to alert the data owners, depending on the type of information stolen. In addition, security measures are required to be taken, depending on the type of stored personal data. Please refer to Section 3 for the regulation that provides the applicable security measures.

3. Law applicable

The applicable laws in Argentina on data protection are the following:

**Law Nº 25,326 (the “Act”)**

**Executive Order Nº 1558/2001.**
Resolutions issued by the Argentine Data Protection Authority. For instance, Disposition No. 11/2006 about “Security Measures for the Processing and Storage of Personal Data Contained in Public Non-State and Private Files, Records, Databases Databanks”; and Disposition No. 4/2009, about “Marketing Activities”.

Disposition No. 11/2006

Disposition No. 4/2009

4. Key Privacy Concepts

a. Personal Data
The Act defines “Personal Data” as information of any kind referring to ascertainable physical persons or legal entities. The Act protects Personal Data used for reporting purposes and recorded in data files, registers, databases or by other technical means.

b. Data Processing
The Act covers the protection of Personal Data with regard to both manual and automatic processing. The Act defines “data processing” as systematic operations and procedures, either electronic or otherwise, that enable the collection, preservation, organization, storage, modification, relation, evaluation, blocking, destruction, and in general, the processing of personal information, as well as its communication to third parties through reports, inquiries, interconnections or transfers.

c. Processing by Data Controllers
The Act defines “Data Processor” as any person - public or private - carrying out, at its sole discretion, data processing, whether contained in files, records, or databases of its own, or through connection therewith. “Data Owner” is defined in the Act as any individual or corporation domiciled in the country, or having offices or branches in the country, whose data is subject to this Act. A Data Controller, a person or organization that holds personal or sensitive information on one or more Data Owners cannot, in principle, process data without the consent of the Data Owners. Nevertheless, under certain circumstances, Data Owner's consent is not necessary. Furthermore, the Act covers all private persons creating files, records or databases that are not intended exclusively for personal use.

d. Jurisdiction/Territoriality
The Act applies to any physical person or legal entity having a legal domicile, or local offices or branches in Argentina. Registers, data files, databases or databanks that are interconnected through networks at inter-jurisdictional, national or international level fall within the federal jurisdiction, and are, thus, subject to the provisions of the Act. Other registers, data files, databases or databanks may also fall under provincial jurisdiction. In this regard, some of
the provinces of Argentina have issued regulations for the “habeas data” remedy. Also, several Provinces have adhered to the content of the Act.

e. Sensitive Personal Data

The Act defines “Sensitive Personal Data” as Personal Data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual habits or behavior. The Act provides that Data Owners cannot be compelled to provide Sensitive Personal Data (nevertheless, certain exceptions may apply, such as health-related and union membership information, information which is necessary for employment purposes). It is prohibited to create files, banks or registers storing information that directly or indirectly reveal Sensitive Personal Data.

f. Employee Personal Data

Employees’ Personal Data is likely to include Sensitive Personal Data (e.g., health-related and union-membership information) and non-sensitive Personal Data. Generally, an employer may be entitled to process certain Sensitive Personal Data of its employee without the employee’s consent if and to the extent it is necessary for employment purposes. This occurs, nevertheless, in very specific and limited cases and should be determined on a case-by-case basis. The Act does not set forth when it is “necessary” for the employer to collect Sensitive Personal Data.

5. Consent

a. General

Consent of the Data Owner is generally required prior to the collection, processing and disclosure of Personal Data. The processing of Personal Data is unlawful unless the Data Owner has given his or her express consent in writing, or through any other similar means, depending on the circumstances. The consent must appear in a prominent and express manner. Furthermore, consent must be an informed consent and is revocable by the Data Owner.

Consent shall not be deemed necessary when Personal Data:

- is secured from unrestricted public access sources;
- is collected for the performance of the duties inherent to the powers of the State or in virtue of legal obligations;
- consists of lists limited to name, ID number, tax or social security identification number, profession, date of birth, and domicile; or
- is derived from a contractual, scientific or professional relationship with the Data Owner (e.g., employment relationship) provided that such Personal Data is necessary for the development of or compliance with the terms of such relationship.
is collected by financial entities in connection with transactions performed by the customers of said financial entities.

b. Sensitive Data
The Act requires express consent from Data Owners for the processing of Sensitive Personal Data.

Exceptions to this rule are:

- processing of Sensitive Personal Data for reasons of general interest authorized by applicable laws;
- processing of Sensitive Personal Data for statistical or scientific purposes, provided that Data Owners cannot be identified (dissociation method);
- Sensitive Personal Data referring to records on criminal or other offenses, provided that the same is processed only by competent public authorities within the framework established by applicable laws and regulations; or
- processing of Sensitive Personal Data relating to the physical or mental condition of patients by public or private health institutions, and medical science professionals, in pursuance of the principles of professional secrecy.

c. Minors
There is no provision that specifically addresses consent requirements for minors. In general, consent cannot be obtained from minors, but can be given by a legal guardian or parent. The Comprehensive Protection of the Rights of Children and Teens Act No. 26,061 prohibits the exposure, circulation and/or disclosure of personal data and images of minors in any medium without consent from the minor and its parents, tutors or legal representatives, when such actions may affect the dignity of reputation of the minors or are intrusive to their private life.

d. Employee Consent
There is no provision that specifically addresses consent requirements for employees.

e. Online/Electronic Consent
In Argentina, electronic consent is permissible and can be effective if properly structured and evidenced.

6. Information/Notice Requirements
An organization that collects Personal Data must provide Data Owners with information about the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; third parties to which the organization will disclose the Personal Data; the consequences of not
providing consent; the rights of the Data Owners; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to contact the privacy officer or other person who is accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; and how to access and/or correct the Data Owners’ Personal Data.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected.

8. Rights of Individuals

Data Owners have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Owner; access the Data Owners’ Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Owners’ Personal Data; request the deletion and/or destruction of the Data Owners’ Personal Data; and exercise the writ of habeas data.

9. Registration/Notification Requirements

The Act states that any public or private “data file, register or database intended to provide reports must be registered with the registry to be established for such purpose.” The Argentine Data Protection Authority has extended the registration requirement to encompass not only data collected in order to provide reports, but also all data collected for purposes beyond personal use.

10. Data Protection Officers

Organizations are required to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization. According to the criteria adopted by the Data Protection Authority, such officer or individual must be located in Argentina.

11. International Data Transfers

The transfer of Personal Data to a third country may take place only if such third country provides similar levels of protection as the ones established by Argentine Law. Exceptions to this requirement are:

- consent of Data Owners;
- execution of an international data transfer agreement by and between the data exporter and the data importer, in accordance with certain guidelines issued by the Argentine Data Protection Authority;
- international judicial cooperation;
• exchange of medical information when so required for the treatment of the Data Owner;
• exchange of medical information required for epidemiological research, provided that Data Owners cannot be identified (dissociation method);
• stock exchange or banking transfers in pursuance of the applicable laws;
• when the transfer is agreed upon within the framework of international treaties signed by Argentina; or
• When the transfer is made for international cooperation purposes between intelligence agencies in order to fight against organized crime, terrorism and drug-trafficking.

12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

The Argentine Data Protection Authority has approved three different levels of security measures that the person responsible for a database shall enforce depending on the type of Personal Data that is processed in such database. The different levels of technical and organizational security measures are the following: (i) basic level (for processors of general Personal Data); (ii) medium level (for utilities, government agencies or private entities that must keep their data secret); and (iii) critical level (for entities processing Sensitive Data). The technical and organizational security measures should include the procedure to be followed by the company in case Personal Data stored in the database is stolen.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and are required to comply with sector specific requirements. Organizations shall be liable together with third party providers in case of breach by the latter.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings, and/or private rights of action. Furthermore, the Argentine Data Protection keeps a record of infractions that is publicly available, so reputational damages may also exist.
15. Data Security Breach

There is no specific mandatory obligation under the current applicable regulations to notify the Argentine Data Protection Authority of a security breach.

From a practical standpoint, when a security breach occurs and becomes public, the Argentine Data Protection Authority usually initiates an investigation to confirm whether the company affected by the security breach has adopted the security measures required by the Act and regulations enacted by the Authority.

There is also no obligation under the Act to notify consumers about a security breach. Nevertheless, companies affected by a security breach usually consider reporting the incident to Data Owners to allow them to adopt the appropriate course of action to protect their information and minimize damages. For instance, when the incident affects information related to any password or similar private information used by its employees, the company should report the incident to the affected employees to allow them to adopt the appropriate course of action (e.g., change of the password).

16. Accountability

Organizations are required to conduct trials prior to the implementation of new information systems and/or technologies, which shall not be performed directly into databases containing Personal Data, unless such organizations have adopted the necessary security measures required by local regulations.

17. Whistleblower Hotline

Whistle-blower hotlines may be established in Argentina as long as they are in compliance with local laws. If an organization plans to create a database with the information received as a consequence of the implementation of a whistle-blower hotline, such database will have to be registered with the Authority. Furthermore, employees will have to be duly informed about the existence of the whistle-blower hotline and relevant policies in relation thereto.

18. E-Discovery

The process whereby electronically-stored information is reviewed, processed and presented for the purposes of litigation or regulatory requests is recognized under Argentine Law. Electronic information can be stored in databases as structured content, in emails or instant messages as semi-structured content, and in documents or files as unstructured content. Nevertheless, employers should advise employees about the implementation of an e-discovery system and the fact that computer use in the workplace (e.g., e-mail, Internet) is being monitored and that information such as e-mails will be stored. Nevertheless, employees may request the employer to destroy any Personal Data stored as a consequence of the implementation of the
e-discovery system. The employer may justify its position by alleging that such information is crucial for complying with regulations and/or for purposes of litigation.

19. Anti-Spam Filtering

The main issues relate to how the spam-filtering solution is implemented, (e.g., whether the spam-filtering solution is automatic and applicable in the same manner to all of the employees and whether it allows certain IT officers of the company to monitor for spam). In practice, companies have installed software that filters spam and automatically sends a list of all of the spam that was filtered by the system to the relevant employee.

20. Cookies

The use of cookies and web beacons would be, in principle, permitted provided that proper notice on their use is given to users (e.g., in the privacy policy). In this regard, the terms and conditions of the privacy policy should indicate that by accepting said terms and conditions, the users accept the deployment and use of cookies and web beacons. It is also recommendable that the privacy policy describes the manner in which the cookies can be deactivated (i.e., from browsers) and the consequences for doing so.

21. Direct Marketing

As regards Direct Marketing performed by fixed or mobile phones, same is regulated by the so-called Do Not Call regulations, according to which those individuals or legal entities that promote products or services through telemarking activities are prohibited from contacting any number registered with the list, and are required to search the registry at least once every 30 (thirty) days and update their internal call list accordingly. As regards online direct marketing, when engaging in direct marketing using various electronic channels, companies should ensure that consumers are given the freedom to choose whether or not to engage in a relationship or receive communications from companies. In addition, the messages provided through electronic means should also contain a transcription of certain articles from the Data Protection Law and its Executive Order.
Australia

Anne-Marie Allgrove
Sydney
Tel: +61 2 8922 5274
anne-marie.allgrove@bakermckenzie.com

Patrick Fair
Sydney
Tel: +61 2 8922 5534
patrick.fair@bakermckenzie.com

Adrian Lawrence
Sydney
Tel: +61 2 8922 5204
adrian.lawrence@bakermckenzie.com

Toby Patten
Melbourne
Tel: +61 3 9617 4456
toby.patten@bakermckenzie.com
1. Recent Privacy Developments

The key legislation regulating privacy in Australia is the Privacy Act 1988 (the “Privacy Act”). Significant amendments to the Privacy Act were passed on 29 November 2012 and came into effect on 12 March 2014.

Since these reforms, there has not been any significant new privacy-related legislation in Australia and there have not been any determinations or case law made under the new law (although there have been a number of privacy assessments and one enforceable undertaking).

The regulator, the Office of the Australian Information Commissioner (OAIC), has released various guidelines in the meantime. The key guidelines are:

- **APP Guidelines** - this provides practical guidance on the application and interpretation of the Australian Privacy Principles (APPs).

- **Guide to developing an APP privacy policy** - this sets out a step by step process to assist organisations in complying with APP 1 which relates to the creation of an organisation’s privacy policy.

- **Guide to undertaking privacy impact assessments** - a privacy impact assessment identifies how a project can affect an individual’s privacy and formalizes recommendations for minimizing the impact. This guide sets out 10 steps to planning a privacy impact assessment.

- **Data breach notification guide** - the guide suggests steps to take once an organization becomes aware of a data breach and states that it may be a reasonable step (pursuant to APP 11- security of personal information) to notify individuals and the regulator of a data breach and provide relevant information.

- **Guide to securing personal information** - this guide sets out practical steps for organisations to appropriately protect the personal information that they hold e.g., the circumstances to consider when formulating reasonable steps, the internal processes to put in place.

- **Handling privacy complaints** - this guide details the regulator’s approach to handling complaints (the commissioner can make enquiries into the matter, investigate, and/or attempt to conciliate, and may also decline to investigate complaints.)

- **Privacy management framework** - this guide sets out steps that the regulator has indicated it expects organisations to take to ensure their compliance with the APPs, including with respect to internal processes, culture, and response to complaints.
2. Emerging Privacy Issues and Trends

- **Data breach notification** - although organisations are not currently required to notify individuals or the regulator of a data breach, legislation to require this has been foreshadowed as being implemented before the end of 2015. The regulator has already released guidelines regarding how organisations should deal with data breaches (see Section 1 above).

- **Increase in privacy complaints** - the regulator has indicated that there has been a significant increase in complaints since the reforms were implemented and that these have been generally due to increased access to personal information, more complex business relationships, direct marketing, data breaches and disclosure of health information.

- **Stricter view towards hacking incidents defence** - the regulator has also indicated that it is not sufficient to use being hacked as an excuse if the organization has not implemented appropriate security protections.

3. Law Applicable

The key privacy legislation in Australia is the Privacy Act which applies to the private sector and Commonwealth public sector. The key data-handling principles applicable to both the private and public sectors sector are contained in the thirteen APPs.

The APPs are grouped into five sets of principles intended to reflect the “life cycle” of handling of personal information. They cover:

- the practices, procedures and systems that entities have in place relating to how they handle personal information;
- how entities collect personal information, including unsolicited personal information;
- how entities manage personal information, including how they use and disclose personal information, disclose information overseas, and how they use Government identifiers;
- how entities ensure the integrity, quality and security of personal information; and
- how entities deal with requests for access to, and correction of, personal information;
**APP Guidelines:** The regulator responsible for the Privacy Act, the Office of the Australian Information Commissioner (“OAIC”) has issued guidelines to provide further context to the APPs.

Some states and territories have privacy legislation and/or administrative guidelines which apply to the State/Territory public sector.

Victoria and New South Wales also have specific legislation governing the collection, storage, use and transfer of health information (the *Victorian Health Records Act 2001* and the *New South Wales Health Records and Information Privacy Act 2002*), which applies in addition to the applicable APPs. "Health information" is broadly defined as personal information about the physical or mental health or a disability of an individual, or information relating to the provision of health services, the donation of body parts or substances, or genetic information that could be predictive of the health of an individual or their relatives.

To the extent that an organization collects, uses, stores or discloses health information, it will be subject to the Health Privacy Principles, which require consent in Victoria and notification in New South Wales when that health information is collected and which restrict trans-border data flows out of the State, except in limited circumstances.

The Australian Capital Territory also has health specific legislation, the *Health Records (Privacy and Access) Act 1997*, which covers health records held in the public sector in the Australian Capital Territory. This legislation also seeks to apply to acts or practices in the private sector to the extent not covered by the Privacy Act.

Finally, Victoria and the Australian Capital Territory also have human rights legislation, which includes a right for individuals not to have their privacy interfered with unlawfully or arbitrarily.

The responses below relate specifically to the obligations in the Privacy Act that are applicable to private and Commonwealth public sector entities.

4. **Key Privacy Concepts**

a. **Personal Data**

“Personal information” is defined in the Privacy Act as “information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.”

The APP Guidelines provide that the concept of information being “reasonably identifiable” can include information which is not “personal information” in its own right, can still come under the Privacy Act if there is a likelihood of it
being combined with other information held by an organisation which would enable an individual to be reasonably identifiable.

b. Data Processing
The APPs in the Privacy Act apply to the acts and practices of entities in respect of personal information, including in relation to open and transparent management of personal information (including clear and technology neutral privacy policies), anonymity, collection of solicited and unsolicited information, notification of collection, use, disclosure, direct marketing, cross-border disclosure, use of government related identifiers, quality and security of the information held and access and correction of information held. The EU definition of “processing” is not used in the Privacy Act. The Privacy Act applies to personal information held in hard-copy and electronically and to both manual and automated handling of data.

c. Processing by Data Controllers
The Privacy Act applies to entities that undertake any of the acts or practices covered by the APPs. No distinction is made between entities that control the personal information and those that process it on behalf of other entities.

d. Jurisdiction/Territoriality
Subject to certain exemptions (see below), the Privacy Act applies to acts and practices:

- done in Australia in relation to personal information by an entity that is subject to Australian law (other than State or Territory Authorities); and
- done outside of Australia in relation to personal information of an Australian citizen or person living in Australia by an entity that either has a link to Australia (such as being a Commonwealth government agency, a partnership formed in Australia or a body corporate incorporated in Australia) or that carries on business in Australia (including by having an online presence in Australia) and collected or held the information in Australia at the time of the act or practice.

The Privacy Act contains a number of exemptions, including in respect of acts or practices:

- of individuals only for the purpose of or in connection with their personal, family or household affairs, or otherwise other than in the course of a business carried on by that individual;
- of small businesses with a turnover of AUD$3 million or less (except those who are related to an entity that has a turnover greater than AUD$3 million, who provide a health service, or who satisfy other criteria specified in the Privacy Act);
- relating to employee records (see Section 4(f) below for further detail); or
undertaken overseas and that are required by foreign laws.

e. Sensitive Personal Data

“Sensitive information” is personal information relating to racial or ethnic origin, political opinions, membership of a political association, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices, criminal record, biometric information or health information.

Pursuant to APP 3, an entity must not collect sensitive information unless:

- the entity obtains the consent of the individual (see Section 5(a), below for further detail) and the information is reasonably necessary for the activities or functions of the entity;

- collection is required by law;

- collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where it is unreasonable or impracticable to obtain the consent of the individual to whom the information relates;

- the information is collected by a non profit organization and relates to the organizations activities and relates solely to the organization’s members or persons who have regular contact with the organization in connection with its activities;

- collection is necessary for the establishment, exercise or defense of a legal or equitable claim;

- where the entity is a Commonwealth enforcement body, the collection is necessary for the performance of that enforcement body’s functions or activities;

- the information is collected in the process of providing a health service, and is either collected as authorized by law or subject to a professional code of ethics; or

- the information is collected in the course of medical research that is subject to professional safeguards and where obtaining consent is impracticable, and the research cannot be performed without the information being collected.

Unless consent is given for an additional use, sensitive information may only be used for the purpose for which it was collected or for a secondary purpose directly related to the purpose of its collection that the individual would reasonably expect the information to be used for.
f. Employee Personal Data

Employee records are given a limited exemption from coverage under the Privacy Act, to the extent applicable to a private organization (as opposed to a Commonwealth public sector agency). This exemption effectively allows private employers to use information concerning their employees for appropriate internal purposes. Three requirements need to be satisfied for the exemption to apply:

- the organization is acting in its capacity as a current or former employer of an individual;
- the use of employee information is directly related to a current or former employment relationship between the employer organization and the individual; and
- the use of employee information is directly related to an employee record held by the employer organization and relating to the individual.

For the exemption to apply, the individual and the organization must be or have been in an employment relationship. The Privacy Act does not define the scope of employment, but it is accepted that this exemption does not extend to contractors, subcontractors, consultants and company directors, all of whom are outside of the employment relationship. Future or prospective employment relationships also do not fall within the exemption, which means that recruitment processes and recruitment agencies must comply with the Privacy Act. The exclusion of both recruitment processes and contractors has the practical effect of requiring human resources processes to implement privacy principles in at least some areas of their handling of personal information.

The use of employee information must be directly related to the employment relationship and also must be directly related to employee records held by the employer. This is intended to prevent employers from using employee records for commercial purposes unrelated to the employment relationship or exploiting the employee records exemption for commercial purposes.

The employee records exemption only applies to employee records held by the employer and does not continue if the employee records are disclosed by the employer to another organization. For example, if records containing personal information about an employee are disclosed to the employer’s insurer for the purposes of workers’ compensation insurance, then those records do not retain their exempt status in the hands of the insurance company. That is, in the hands of the insurance company, the personal information is subject to the coverage of the Privacy Act.

g. Data handling practices

Entities are required to take reasonable steps to implement practices, procedures and systems to ensure that they comply with the APPs and can
deal with inquiries or complaints about their compliance with the APPs. This principle is intended to keep the Privacy Act up-to-date with international trends and encourage entities to ensure that privacy compliance is included in the design of information systems, goods and service offerings from their inception. An organization is expected to take an active role in monitoring its privacy handling practices, including determining whether information it holds is still required for the purposes for which it was collected, the accuracy of that information and whether the use of identifiable information is necessary for an organisation’s intended purposes or if de-identified information could instead be used. Information which is no longer required should be destroyed or de-identified.

5. Consent

a. General

There is no express requirement for an entity to obtain an individual’s consent to collect personal information so long as the entity only uses that information for the purpose for which it was collected or for a related purpose (or directly related secondary purpose in the case of Sensitive Data) that the individual would reasonably expect the information to be used for. Except in limited circumstances, an entity must obtain the individual's consent to use the Personal Data for any other purpose.

Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is usually understood to only cover the identified purpose(s).

There is no mandatory requirement that consent must be in writing for it to be valid. It can be usually provided orally or in different forms and formats. The Data Subject also has the right to withdraw consent at any time.

In addition, consent does not need to be in the local language provided that the Data Subject understands the language in which consent is given.

b. Sensitive Data

Australian law recognizes Sensitive Data as a special category of Personal Data. It is therefore subject to additional and special consent requirements. In non-binding guidelines, the Privacy Commissioner expressed the view that an entity would ordinarily need clear evidence that an individual had consented to it collecting Sensitive Data. (See Section 5(a)).
c. **Minors**

While consent from minors is not specifically addressed in the Privacy Act, the Privacy Commissioner has expressed the view through non-binding guidelines that organizations should consider in each case whether an individual has capacity to give consent and, “as a general principle, a young person is able to give consent when he or she has sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person.”

d. **Employee Consent**

In Australia, there are some doubts as to whether consent given in the context of an employment relationship can be considered valid. It is questionable whether consent would qualify as voluntary, given that the employee may feel forced to consent due to the subordinate nature of their relationship with their employer. Consent has also been construed as misleading where statutory permission to collect, process, and use Personal Data is available. As a matter of practice, in order for such consent to be valid, the employer may need to be able to demonstrate that the employee had a genuine option not to consent. This issue arises less commonly under the Privacy Act because of the limited employee records exemption for some aspects of employee record processing (See Section 4(f)).

e. **Online/Electronic Consent:**

In Australia, online or electronic consent is permissible and deemed effective if it is properly structured and evidenced.

6. **Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity; if Personal Data is collected from a third party or if the Data Subject is not aware that the organization has collected the Personal Data, the fact that the organization has collected that Personal Data and the circumstances of the collection; if the collection is required or authorized by Australian law or court order, the fact that the collection is required by that law or court which issued the order; the types of Personal Data being collected; the purposes for collecting Personal Data; that the organization has a privacy policy containing information on how the Data Subject may access Personal Data about the Data Subject and seek correction, and associated complaint processes; third parties to which the organization will disclose the Personal Data; the consequences to the Data Subject if the Personal Data is not collected; and whether the Personal Data is likely to be disclosed outside of Australia, and if so, to which countries (if known and practicable to specify those countries).
7. Processing Rules

An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; anonymize the Personal Data whenever possible; provide the Data Subject the option to use a pseudonym or remain anonymous whenever possible; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; and, request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

An organization that collects and processes Personal Data are not required to register, file and notify the appropriate data authority.

10. Data Protection Officers

In Australia, there is no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization. However, organizations are required to make available a privacy policy on request from a Data Subject. (See Section 1.)

11. International Data Transfers

If an organization discloses Personal Data to a recipient outside of Australia, it must take reasonable steps to ensure that the recipient does not breach the APPs. Unless an exception applies, if the recipient handles the Personal Data in a manner that would breach the APPs if that recipient were subject to the APPs, the organization that disclosed the information will be taken to have breached the APPs. A key exception is if the recipient to which Personal Data is disclosed is subject to a law or binding scheme which provides the same protection as under the Privacy Act, and there are mechanisms that the Data Subject can access to enforce that law or binding scheme. A further exception is if the organization expressly informs Data Subjects that if information is disclosed outside of Australia, the organization will not be responsible for any failure of the recipient to protect the Personal Data in a manner consistent with the APPs, and having been so informed the Data Subject consents to the disclosure.

Safe Harbor registration may assist in establishing that reasonable steps have been taken if the organization applied Safe Harbor principles to Personal Data from Australia.
12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties may be required to use contractual or other means to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors. In case of an occurrence of data breach, the outsourcing organization may be held liable together with the third party provider.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, class actions, and/or private rights of action.

15. Data Security Breach
Although currently there is no legal requirement in Australia for organizations to notify Data Subjects when a privacy breach occurs, this is an area of focus for the OAIC and the OAIC has issued voluntary guidelines regarding data breach.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions and/or class actions if it has breached the APPs.

16. Accountability
The changes to the Privacy Act are in many ways non-prescriptive, and put the onus on an organization to develop its systems such that privacy compliance is a key consideration. The OAIC has stated that “establishing a comprehensive and practical privacy policy … will get you started with a ‘privacy by design’ approach to your business”, and further recommends that organizations look closely at their information security and data breach plans as against the new laws. Finally, it is also recommended that organizations conduct privacy impact assessments for new projects. The OAIC has issued a “Privacy Impact Assessment Guide” to assist organizations.
17. Whistle-blower hotline

Whistle-blower hotlines may be established in Australia provided that they are in compliance with local laws.

18. E-discovery

When implementing an e-discovery system, an organization may be required to: obtain the consent of employees if the collection of personal data is involved; and advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.

20. Cookies

There are no specific laws/rules that regulate the use and deployment of cookies in Australia. In general, the use of cookies must comply with data privacy laws. As such, consent of Data Subjects may have to be obtained before cookies can be used.

21. Direct Marketing

Whether businesses can use Personal Data for direct marketing will depend on how they collected the information (whether it was directly from the relevant Data Subject or from a third party) and whether individuals would reasonably expect their information to be used for this purpose. There is also a new opt-out requirement that applies to all direct marketing communications. Additional restrictions apply to the use of Sensitive Data for direct marketing. In an on-line context, the APP Guidelines provide an example that direct marketing may include the display of an advertisement on a social media site that an individual is logged into where those advertisements are tailored based on that individual’s browsing history, but not where advertisements appear uniformly to any browser of that website.
Austria

Lukas Feiler
Vienna
Tel: +43 1 24250 450
lukas.feiler@bakermckenzie.com
1. Recent Privacy Developments

The Data Protection Amendment Act 2014, which was passed in May 2013 and entered into force on 1 January 2014, transformed the Data Protection Commission to a monocratic agency and renamed it the Data Protection Authority ("Authority"). Appeals against decisions by the Authority will now have to be lodged at the Federal Administrative Court, which was created by the Administrative Judicial Reform 2012.

2. Emerging Privacy Issues and Trends

**Internal compliance investigations** – Internal compliance investigations are becoming more common, particularly with potential competition law enforcement actions and leniency applications. The requirements concerning the confidentiality and swiftness of such investigations pose significant challenges under Austrian data protection law, in particular if the investigation entails the review of corporate and private emails sent or received via corporate email accounts. Practice has shown that compliance risks can only be mitigated to acceptable levels if certain technological safeguards are implemented in the forensic process.

**Big Data** – The use of analytics applications in analyzing huge amounts of typically unstructured data has significant economic potential for any enterprise and also brings with it serious data protection compliance challenges regarding the principle of purpose limitation. To address these challenges, data protection should be considered early on when designing Big Data applications and the associated (automated) decision processes.

3. Law Applicable

The amended Austrian Federal Data Protection Act 2000 (*Datenschutzgesetz*) (the “DSG”), effective as of 1 January 2000, implementing the Data Protection Directive 95/46/EC and last amended by the Data Protection Amendment Act 2014, which was passed in May 2013 and entered into force on 1 January 2014.

4. Key Privacy Concepts

**a. Personal Data**

The DSG applies to information relating to Data Subjects who are identified or identifiable (individuals and legal persons) (the “Data Subject”).

**b. Data Processing**

“Processing of data” means collecting, recording, storing, keeping, sorting, comparing, modifying, linking, reproducing, culling, disseminating, utilizing, committing, blocking, deleting, destroying or any other kind of handling of data, with the exception of the transmission of data.
“Transmission of data” is the transfer of data to recipients other than the Data Subject, the Controller or a Processor, in particular publishing of such data as well as the use of data for another application or purpose.

“Committing of data” is the transfer of data from the Controller to a Processor.

“Use” describes any kind of handling of data, therefore includes both the processing and the transmission of data.

c. Processing by Data Controllers

The DSG applies to the party responsible for the purposes and the manner that Personal Data is to be used (“Data Controller”). If the Data Controller outsources processing activities to a third party (a “Processor”), that Processor is subject to the DSG as well.

d. Jurisdiction/Territoriality

The DSG applies to:

- Data Controllers established in Austria;
- Data Controllers established outside Austria, but within an EU Member State, that use Personal Data for an establishment that the Data Controller has in Austria;
- Data Controllers not established in any EU Member State which use Personal Data in Austria.

e. Sensitive Personal Data

The DSG imposes additional requirements for the use of special categories of Personal Data (“Sensitive Personal Data”) – that is, data relating to natural persons concerning their racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, health and sexual life. Specifically, the use of Sensitive Personal Data is prohibited, unless certain conditions are met, including:

- the Data Controller obtains the explicit and unambiguous consent of the Data Subject (see Section 5(b) below);
- the use is necessary to protect the vital interests of the Data Subject or of a third party where the Data Subject is physically or legally incapable of giving consent;
- the data has evidently been made public by the Data Subject himself or herself;
- the use is necessary in order to assert, exercise, or defend legal claims, and there is no reason to assume that the Data Subject has an overriding legitimate interest in excluding the use;
• the use is necessary for the purposes of scientific research, and the scientific interest in carrying out the research project substantially outweighs the Data Subject’s interest in excluding use, and the purpose of the research cannot be achieved in any other way or would otherwise necessitate a disproportionate effort;

• the use is necessary for medical purposes and the processing is undertaken by a health professional or person with the equivalent duty of confidentiality as a health professional; or

• the use is required in view of the Data Controller’s rights and obligations in connection with labor or employment law and is admissible pursuant to special legal provisions, whereby the rights of the works council relating to the use remain unaffected.

f. Employee Personal Data

Employee Personal Data is likely to include Sensitive Personal Data (e.g., health-related information, religious denomination) and Personal Data.

An employee’s Sensitive Personal Data generally may only be processed with the employee’s explicit consent (as the other circumstances mentioned in Section 4(e) above will usually be irrelevant in a standard employment relationship), unless specific statutory rules (other than the DSG) otherwise allow the processing of such data, as is the case, e.g., with respect to information regarding religious denomination for church tax reasons (pursuant to relevant tax provisions).

An employee’s Personal Data may be processed by a Data Controller in certain circumstances, including if the processing activities are necessary for the performance of the employment contract – i.e., if: (i) they are required for the fulfillment of primary or collateral contractual or pre-contractual duties; or (ii) they are necessary to safeguard justified interests of the Data Controller and there is no reason to assume that the employee has an overriding legitimate interest in his or her Personal Data being excluded from processing or use.

A fallback justification for processing of both Sensitive Personal Data and Personal Data in the employment context is the provision of consent by the Data Subject. However, it is debatable whether consent can be validly given in the employment context (see Section 5(d) below).

5. Consent

a. General

Consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances.
Consent is contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to only cover the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

There is no requirement that consent must be in writing. It can be provided orally or in different forms and formats. In addition, the Data Subject also has the right to withdraw consent at any time.

Generally, consent must be in the local language to be valid. However, it may be considered valid consent even if it is not in the local language if the Data Subject understands the language in which consent is given.

b. Sensitive Data

Austrian law recognizes Sensitive Data as a special category of Personal Data. It is subject to additional and special consent requirements. While Sensitive Data may only be collected and processed with the express consent of the Data Subject, Sensitive Data may be processed without obtaining consent in certain prescribed circumstances.

c. Minors

While consent from minors is not specifically addressed in any law, the general rule is that minors are considered incapable of giving consent. However, parents or legal guardians of minors are allowed to provide consent on behalf of the minor, and may even be allowed to obtain information about the minor from third parties without the need of consent from the minor. Nevertheless, there are certain circumstances where consent given by a minor may be considered valid.

d. Employee Consent

In Austrian legal literature, there are doubts as to whether consent given in the context of an employment relationship can be considered valid. First, it is questioned whether the consent would qualify as voluntary, given that the employee may feel forced to consent due to the subordinate nature of their relationship with their employer.

Secondly, it has been held that consent would be misleading where statutory permission to collect, process, and use Personal Data is available.

Therefore, a consent declaration is only considered unproblematic if the declaration of intent is based on a free decision. In a relationship of dependence such as an employer-employee relationship, this freedom of decision can be significantly restricted, potentially making consent declarations by employees problematic.
In any case, where a works council exists, the conclusion of an agreement with that works council regarding the employee data processing is typically required.

The general rule is that employee consent is required to collect and process an employee’s Personal Data; however, there are instances when employee consent is not required, e.g., to carry out an employment contract or administer an employment relationship, or to fulfill a legitimate interest of the employer.

e. **Online/Electronic Consent**

In Austria, online or electronic consent is permissible and deemed effective if properly structured and evidenced.

6. **Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity, the purposes for collecting Personal Data, the consequences of not providing consent, and the rights of the Data Subject.

7. **Processing Rules**

An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; anonymize the Personal Data whenever possible; provide the Data Subject the option to use a pseudonym or remain anonymous whenever possible; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. **Rights of Individuals**

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. **Registration/Notification Requirements**

Though not mandatory, an organization that collects and processes Personal Data may be required to register, file and notify the appropriate data authority.
10. Data Protection Officers

In Austria, there is no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

Transfers of Personal Data (the Transmission or Committing of Data) from Austria to other EEA countries are generally permitted without the need for further approval by the Austrian Data Protection Authority, provided that such transfers would be legal within Austria. The same applies with respect to transfers to Canada, Switzerland, the Isle of Man, Argentina, Andorra, New Zealand, Uruguay, Faroe Islands, Israel, Jersey, and Guernsey, which are subject to European Commission findings of adequacy (subject to the fulfillment of certain pre-conditions) in relation to their data protection laws.

Transfers to the U.S. are permitted without prior approval by the Authority where the recipient has registered under the Safe Harbor arrangement and provided that the transfers would be legal within Austria. Transfers to the U.S. or any other countries outside the EEA that do not provide an adequate level of data protection are legal if based on unmodified or modified versions of the relevant EU Model Clauses, provided always that such transfers would be legal within Austria.

However, the Austrian Data Processing Register has to be notified in any case, unless covered by the above mentioned exceptions (covered by a standard application; contain solely published data or data for the management of public registers and catalogues; contain data solely for which neither the Data Controller, any Processor or any recipient can determine the identity of the Data Subject; contain only Personal Data or family data for private purposes or data for journalistic purposes). Furthermore, any transmissions based on the EU Model Clauses also require the prior approval by the Austrian Data Protection Authority.

Transfers of Personal Data to countries outside the EEA may further take place even without additional measures to ensure an adequate level of data protection at the recipient’s end where:

- the Data Subject has consented to the transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller, or to take steps at the Data Subject’s request with a view to entering into a contract with them;
- the transfer is necessary for the performance of a contract between the Data Controller and a third party in the interest of the Data Subject;
- the transfer is necessary for the purpose of establishing, exercising, or defending legal claims before a foreign authority; or
• the Personal Data have been published legitimately in Austria (e.g., available from a public register).

The general rules concerning the legality of processing must always be fulfilled (i.e., the transfer would need to be legal even within Austria).

In all other cases, prior authorization by the Authority is required by law.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organizational security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors. In case of an occurrence of data breach, the outsourcing organization may be held liable together with the third party provider.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

Organizations that are involved in a data breach situation are required to comply with mandatory data breach notification requirements, take steps to contain the breach, and comply with data authority orders and court orders. Depending on the nature and scope of the breach, the organization is not required to notify the data authority. However, the organization may have to notify the impacted Data Subjects in case of a data breach. The organization may be required to gather information about the breach, assess the potential risk of harm to the Data Subjects, take steps to prevent future similar breaches and assist authorities with any investigation relating to the breach.

An organization that is involved in a data breach situation may be subject to a closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, or civil actions and/or class actions.
16. Accountability

There is no existing law in Austria that requires organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. It is also not a requirement to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

17. Whistle-blower hotline

Whistle-blower hotlines may be established in Austria provided that they are in compliance with local laws.

18. E-discovery

When implementing an e-discovery system, an organization is required to advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace, give employees the opportunity to opt-out from the spam-filtering solution, and give employees the opportunity to review the isolated emails designated as spam.

20. Cookies

There are specific laws/rules that regulate the deployment of cookies, and hence, the use of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.
Azerbaijan

Gunduz Karimov  
Baku  
Tel: +994 12 4971 801  
gunduz.karimov@bakermckenzie.com

Jamil Alizada  
Baku  
Tel: +994 12 4971 801  
jamil.alizada@bakermckenzie.com
1. Recent Privacy Developments

The Information Acquisition Law (as defined below) was amended to include information on financial operations within the scope of personal data. Access to such information is restrained.

The State Secrecy Law (as defined below) was amended to introduce the additional conditions on access of officials to state secrets and commitment on non-disclosure thereof and grounds for rejection of such access.

2. Emerging Privacy Issues and Trends

No emerging trends.

3. Law Applicable


4. Key Privacy Concepts

a. Personal Data

The Personal Data Law defines personal data as any information which makes it possible to identify a person directly or indirectly. The Labor Code further includes as personal data general information on an employee, such as his or her name, home address, and any other information reflected in his or her national identification card.

Personal data may be classified as either general or private. Personal information such as a person’s first, second and patronymic name is regarded as general personal data.

The Information Acquisition Law restricts the collection of private information on an individual’s political views, religious affiliation, ethnicity, health and similar matters.
b. Data Processing

The Information Law defines data processing as the creation, collection, processing, storage, search and dissemination of information. The Information Law further regulates data processing through the use of information resources. Resolution 38 establishes rules on data processing applicable to: (i) document storage, systematization and protection; (ii) creation, storage and updating of document registers; and (iii) the use of documents maintained in a register.

c. Processing by Data Controllers

A data controller is a “holder of information” required by law to provide information to the public upon request. Under the Information Acquisition Law, a “holder of information” is defined as including: (i) state and municipal authorities; (ii) public entities (vested with certain social responsibilities); and (iii) legal entities and individuals providing services in the areas of education, medicine and culture. Entities having a dominant position in a particular market are also regarded as “holders of information”.

d. Jurisdiction/Territoriality

The privacy-related laws listed in Section 3 apply to the creation, collection, processing, storage, search, and dissemination of information in Azerbaijan.

e. Sensitive Personal Data

The Information Acquisition Law restricts public access to certain categories of personal data including information: (i) on political views, religion, ideology, ethnic and racial origin; (ii) on health and physical and mental disabilities; (iii) collected during criminal investigations prior to publication in open court hearings; (iv) on social welfare program applications; (v) on previous convictions; (vi) on domestic violence; and (vii) on collected taxes, excluding tax arrears. The Biometric Information Law also restricts public access to biometric information, i.e., information on a person’s intrinsic physical traits such as fingerprints, DNA, face and iris recognition, etc.

The Information Acquisition Law also restricts public access to certain information on family life including data relating to: (i) sex life; (ii) matrimonial and other family matters; (iii) child adoption; and (iv) notarial acts.

f. Employee Personal Data

Employee-related information (i.e., name, residential address and any other information reflected on a national identification card) is personal data. Information on an employee’s salary, title, business address and telephone number, however, is not personal data.
5. Consent Requirements

a. General
Article 32.3 of the Constitution requires the subject’s consent for the collection, processing, storage and dissemination of information relating to the subject’s data.

b. Sensitive Data
Release of personal data relating to the subject without his or her consent is prohibited.

c. Minors
No consent is required to release information on minors (under 18) to their parents, guardians and other legal representatives.

d. Employee Consent
The Labor Code prohibits employers from releasing information relating to its employees without the employees’ consent.

e. Online/Electronic Consent
While the Information Acquisition Law specifically provides for an electronic release of information, it is silent on the availability of “electronic” consent. As a general matter, consent must be in writing (i.e., signed) to be effective.

6. Information/Notice Requirements
Not applicable.

7. Processing Rules
Resolution 38 establishes the processing rules.

8. Rights of Individuals
An individual is entitled to have access to information unless such information is classified. The data subject has also a right to obtain documented personal information without restriction.

The Information Acquisition Law authorizes certain entities and individuals access to personal data including: (i) parents, guardians and custodians – with regard to personal data relating to the children in their custody; and (ii) guardians – with regard to personal data relating to handicapped persons in their custody.

Azerbaijani law provides additional rights, including an individual’s right to: (i) correction of information about himself or herself if information is inaccurate; and (ii) assistance from data controllers in connection with the release of information.
9. Registration/Notification Requirements
A data controller must register in its database: (i) information in its possession, including personal data; and (ii) requests for release of information. No particular notification requirements are established (other than notifications to data controllers to data requesters).

10. Data Protection Officers
The Information Acquisition Law imposes certain obligations on data controllers.

11. International Data Transfers
Under the Personal Data Law, any data transfer, including international data transfers, requires the subject’s written consent. International data transfers are prohibited if they pose a threat to the national security of Azerbaijan or if the laws of a recipient country do not provide the legal protection of personal data afforded to subjects under Azerbaijani law.

12. Security Requirements
Yes. The Information Acquisition Law requires a data controller to ensure protection of personal data.

13. Special Rules for the Outsourcing of Data Processing to Third Parties
It is neither prohibited nor specifically authorized.

14. Enforcement and Sanctions
A violation of Azerbaijani law on document storage, systematization and protection is a misdemeanor. Azerbaijani law subjects individuals, officers and legal entities to a fine up to AZN 25, AZN 90 and AZN 300, respectively.

15. Data Security Breach
Except for the general right of a person to require adequate protection of collected data, Azerbaijani laws do not set legal requirements in the event of a data security breach.

16. Accountability
Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. It is also not a requirement to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.
17. Whistle-blower Hotline
There are no rules/laws in Azerbaijan that govern whistle-blower hotlines.

18. E-discovery system
There are no rules/laws in Azerbaijan that govern e-discovery.

19. Anti-spam-filter
As spam-filtering (often coupled with deleting emails) involves a detailed analysis of email content, it raises a customer’s privacy concern.

20. Cookies
The use of cookies must comply with Azerbaijani laws that relate to privacy.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. The organization may be required to obtain consent for a specific activity as bundled consent may not be considered valid consent.
Belgium

Elisabeth Dehareng
Brussels
Tel: +32 2 639 36 11
elisabeth.dehareng@bakermckenzie.com

Daniel Fesler
Brussels
Tel: +32 2 639 36 11
daniel.fesler@bakermckenzie.com
1. Recent Privacy Developments

Information security: new notification forms for security breaches adopted by the Belgian Privacy Commission and new version of security guidance

Since 2014, Information security has definitely become a must for any processing of Personal Data (defined below) in Belgium, following the recommendations adopted and enforcement actions taken by the Belgian Privacy Commission in 2013.

In 2014, the Privacy Commission issued new electronic notification forms and procedures for the reporting of security breaches (mandatory procedure for telecommunication network or service operators, and non mandatory for others). These forms are available in a new section of the Belgian Privacy Commission’s website dedicated to information security and data breaches.

In December 2014, the Belgian Privacy Commission also adopted a new version (version 2.0) of its Guidelines for the security of personal data, that are applicable to all data processing activities subject to a prior authorization. These Guidelines clearly draw inspiration from the International Standards 27002, 27005 and 27018. Although the Privacy Commission has no power to enact mandatory rules, it is clearly of the view that to comply with such guidelines is part of the data controllers’ and data processors’ legal duty to adopt and implement technical and organizational measures aimed at protecting the security of personal data. By merely replicating certain specifications of the international standard 27002 in its guidelines, the Privacy Commission gives to such specifications the status of state of the art norms in such a way that it will become difficult for data controllers and data processors not to comply with them.

In 2014, the Belgian Privacy Commission and the Dutch Data Protection Authority closed their investigation on the security measures implemented by the Society for Worldwide Interbank Financial Telecommunication (“SWIFT”). SWIFT had already dealt with an investigation from the Belgian Privacy Commission between 2006 and 2008. SWIFT, based in Belgium with an operating center in the Netherlands where traffic data is processed and stored, exchanges standardized financial messages in more than 200 countries every day. The Belgian and Dutch data protection authorities concluded that SWIFT had not infringed data protection requirements regarding European citizens’ financial transaction data.

New guidance regarding privacy at the workplace

In 2014, the Belgian Privacy Commission issued a new brochure summarizing its previous advice and recommendations regarding privacy at the workplace, including issues such as camera monitoring, “Bring Your Own Devices” policies, geolocation of employees, use of biometric data, etc.
Draft recommendation and public consultation on the use of cookies

Following a public consultation in 2014, the Belgian Privacy Commission published its final recommendation on the use of cookies (CO-AR-2012-004) in February 2015. This is the commission’s first official guidance on cookies and similar technologies, and it covers both technical and legal aspects. The recommendation notably provides guidance on the information obligation, the consent requirement and the exemptions thereto, as set forth under the Belgian Electronic Communication Act of 13 June 2005. The Privacy Commission recommends following a granular approach, giving users the possibility to accept all or only certain types of cookies.

Opinions regarding the use of cloud computing by hospitals, use of ‘Dashcams’, drones, right to be forgotten, use of electronic identity cards

In 2014, the Privacy Commission issued a number of opinions and recommendations relating to different matters with privacy implications, such as the use of dashcams in cars, privacy-related questions regarding the use of drones, questions relating to the scope of the right to be forgotten following the Judgment of the EU Court of Justice of 13 May 2014 in Case C-131/12, or the use of Belgian electronic identity cards by private companies for authentication of their employees.

In 2015, the Privacy Commission issued an advice with respect to draft guidelines regarding the use of “cloud” by hospitals (CO-A-2014-053). This opinion covers both the legal and technical aspects regarding the processing and storage of health-related data.

Data transfer agreements: approval process

On trans-border personal data flows, the Privacy Commission and the Belgian Department of Justice adopted a protocol in June 2013 according to which all data transfer agreements had to be submitted to the Belgian Privacy Commission for review and approval. Agreements conforming to the Standard Contractual Clauses adopted by the EU Commission were automatically approved by the Belgian Privacy Commission. Non conforming agreements have to be approved by the King, i.e., the Federal Government.

This Protocol was corrected in June 2014 to clarify that no Royal Decree – nor any other form of authorization – is required for data transfer agreements conforming to the EU Commission Standard Contractual Clauses, which are automatically recognized as offering sufficient guarantees in terms of protection of data subjects’ privacy and fundamental rights and freedoms. The King, i.e., the Federal Government, must still approve non-conforming agreements.
2. Emerging Privacy Issues and Trends

- **Information security requirements** - As outlined above, the main privacy issues and trends initiated in 2014 are again related to data breaches and information security requirements, notably in light of a number of hacking of personal data - including sensitive personal data - reported in the press.

- **Cloud computing** - The privacy issue in relation to the processing and transfer of Personal Data in the cloud computing environment is still a hot topic in 2015, with a new opinion of the Privacy Commission regarding the use of “cloud” by hospitals.

- **New EU data protection framework** - Another important hot topic consists in the revision of the EU data protection framework, particularly around the EU Commission Proposal for a Regulation on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data. On 5 February 2014, the Privacy Commission issued an own-initiative opinion (Opinion No. 10/2014) on the draft regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as voted by the LIBE Committee of the European Parliament on 17 October 2013 (CO-A-2014-001). On 17 June 2015, on its own initiative, the Privacy Commission issued a new opinion (Opinion 23/2015) in view of the trilogue to come on the proposals of European Regulation relating to the protection of individuals with respect to the processing of personal data and free movement of such data as proposed by the EU Commission and adopted by the European Parliament and Council (CO-A-2015-024).

- **IP tracking, behavioral advertising and direct marketing**, particularly the new “Do Not Call Lists”, as well as processing of personal data by social media websites, were also key privacy concerns in 2014 and are very hot topics in 2015 with the first court case initiated by the Belgian Privacy Commission in that respect.

- **Internal investigations and privacy at the workplace** - Key issues also include the development of internal investigations within Belgian companies, and, as the case may arise, at European or worldwide group levels, the processing and transfer of personal data in relation to e-discoveries and forensic reviews, as well as the monitoring and review of employees’ electronic communications data within the context of such investigations.
3. Law Applicable

The applicable law includes the Act of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, as modified by the implementing Act of 11 December 1998 and the Act of 29 February 2003, and as supplemented by the Royal Decree of 13 February 2001 (the “DPA”). Data protection rules may also be found in, e.g., the Criminal Code, the Act of 11 March 2003 on Certain Legal Aspects of Information Society Services, the Electronic Communications Act of 13 June 2005, the Act of 21 March 2007 on Surveillance Cameras and in collective bargaining agreements.

4. Key Privacy Concepts

a. Personal Data

The DPA applies to any information (“Personal Data”) relating to an identified or identifiable individual (“Data Subject”). An identifiable person is one who can be identified directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal Data is not necessarily identifying data.

Data will only be considered ‘anonymous’, and therefore not ‘Personal Data’ in the sense of the DPA, provided that the individual to whom it relates cannot be identified, whether by the Data Controller or by any other person, taking account of all the means reasonably likely to be used either by the controller or by any other person to identify that individual.

b. Data Processing

“Processing” is very broadly defined and will cover any operation or set of operations performed on Personal Data including collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, as well as blocking, erasure, and deletion of Personal Data.

The DPA applies to the processing of Personal Data wholly or partly by automatic means, as well as to manual data processing where the data so processed is recorded in or is intended to form part of a filing system.

c. Processing by Data Controllers

The DPA applies to those persons who, alone or jointly with others, determine the purposes for which and the manner in which any Personal Data is or will be processed (“Data Controller”).
d. **Jurisdiction/Territoriality**

The DPA applies to:

- Data processing activities carried out by Data Controllers established in Belgium; and
- Data processing activities of Data Controllers that are not established in the EU but that use equipment based in Belgium to carry out data processing activities (other than merely for transit purpose).

The DPA therefore applies independently of the nationality/residence/location of the Data Subjects whose data are being processed.

e. **Sensitive Personal Data**

The DPA imposes additional requirements for the processing of sensitive Personal Data, i.e., data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, data concerning sex life, as well as health-related data.

Pursuant to Article 6 of the DPA, the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership as well as data concerning sex life is prohibited unless:

a. the Data Subject has given his written consent to the processing, it being understood that such consent can be withdrawn at any time (see Section 5(b) below);

b. the processing is necessary for the purpose of carrying out the specific obligations and rights of the Data Controller in the employment field;

c. the processing is necessary to protect the vital interests of the Data Subject or another person, provided that the Data Subject is physically or legally incapable of giving his consent;

d. the processing relates to Personal Data that has obviously been made public by the Data Subject;

e. the processing is necessary for social security purposes;

f. the processing is necessary for the establishment, exercise or defense of legal claims;

g. the processing is necessary for scientific research and carried out under the terms established by the King in a decree agreed upon in the Council of Ministers after advice of the Commission for the protection of privacy;

h. the processing is carried out in pursuance of the law of July 4, 1962 on public statistics; or

i. the processing is made mandatory by law, decree, or ordinance, or another important reason of public interest, etc.
Pursuant to Article 7 of the DPA, the processing of health-related data is prohibited unless:

a. the Data Subject has given his or her written consent to the processing, it being understood that such consent can be withdrawn at any time;

b. the processing is necessary for the purpose of carrying out the specific obligations and rights of the Data Controller in the employment field;

c. the processing is necessary for social security purposes;

d. the processing is made mandatory by law, decree, or ordinance, or another important reason of public interest;

e. the processing is necessary to protect the vital interests of the Data Subject or of another person, provided that the Data Subject is physically or legally incapable of giving his or her consent;

f. the processing is necessary for the prevention of an actual danger or the suppression of a specific criminal offense.

g. the processing relates to Personal Data that has obviously been made public by the Data Subject; or

h. the processing is necessary for the establishment, exercise or defense of legal claims, etc.

Additionally, pursuant to Article 7, § 4, of the Data Protection Act, health-related data can only be processed under the responsibility of a health care professional, except where the written consent of the Data Subject has been obtained or if the processing is necessary for the prevention of an actual danger or the suppression of a specific criminal offense.

It is worth noting that Article 42, § 2, of the Act of 13 December 2006 containing various health provisions provides that the communication of any Personal Data relating to health is subject to an authorization of principle of the Health Section of the Sector Committee of Social Security; specific exemptions may apply.

Furthermore, the processing of judicial data, including Personal Data relating to litigations that have been submitted to courts as well as administrative judicial bodies, regarding suspicions, persecutions or convictions in matters of criminal offenses, administrative sanctions or security measures, is also prohibited in principle, unless such processing is performed:

- under the supervision of a public authority or ministerial officer, if processing is necessary for the performance of their tasks;
- by other persons, if processing is necessary for the realization of objectives that have been laid down by or by virtue of a law, decree, or ordinance;
by natural persons or private or public legal persons, as far as necessary for the management of their own litigations;

by attorneys at law or other legal advisers, as far as necessary for the protection of the interests of their clients; or

where the processing is necessary for scientific research and carried out under the conditions established or laid down by royal decree.

Persons authorized to process such Personal Data shall be subject to secrecy obligations.

Under Belgian law, an employer (current or potential) cannot rely on its employees’ written consent to process their sensitive Personal Data, except where the processing aims to grant them an advantage. The same applies if the Data Subject is in a dependent position with respect to the Data Controller, preventing the Data Subject from giving his or her free consent.

Lastly, additional security measures apply to the processing of sensitive Personal Data (in addition to the security requirements applying to all data):

a. the categories of persons having access to the Personal Data must be designated by the Data Controller, or, as the case may arise, by the Data Processor, with a detailed description of their function with respect to the processing of sensitive Personal Data;

b. a list of categories of the designated persons must be put at the Privacy Commission’s disposal by the Data Controller or, as the case may arise, by the Data Processor;

c. the designated persons must be held, by a legal or statutory obligation, or by an equivalent contractual provision, to preserve the confidential character of sensitive Personal Data;

d. when informing the Data Subject about the processing of his or her data, the Data Controller must mention the act or regulation authorizing the processing;

e. if the processing is only authorized with the Data Subject’s written consent, the Data Controller must inform the latter of the reasons for the processing and provide him or her with a list of the categories of individuals having access to the Personal Data.

Non sensitive Personal Data may be processed if at least one of the following preconditions is met:

a. the Data Subject has unambiguously given his or her consent to the processing (although there are some concerns regarding consent given in the employment context - see Section 5(d) below);
b. the processing is necessary for the performance of a contract to which the Data Subject is a party or for the performance of pre-contractual measures taken at the request of the Data Subject;

c. the processing is necessary for compliance with an obligation to which the Data Controller is subject by or by virtue of law (to be understood as Belgian law);

d. the processing is necessary in order to protect the vital interests of the Data Subject;

e. the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed;

f. the processing is necessary for the purposes of the legitimate interests of the Data Controller or of the third party to whom the data is disclosed, provided that such interest is not overridden by the Data Subjects’ fundamental rights and freedoms.

f. Employee Personal Data

Employee Personal Data is likely to include sensitive Personal Data (e.g., trade union membership or health-related information) and non sensitive Personal Data. Sensitive employee Personal Data may only be processed in the circumstances mentioned in Section 4(e) above and, in particular, for the purpose of carrying out the Data Controller’s specific rights and obligations under employment law.

For instance, employers must process data with respect to leaves of absence of their employees in order to allow the due payment of social security indemnities. However, employers are not entitled to record the nature of illnesses affecting their employees. It must be stressed that, in Belgium, such processing operations are generally performed by the so-called “Secrétariats sociaux”, i.e., external service providers that manage the payrolls of their clients.

Additionally, trade union membership data may only be processed by the employer for the purpose of payment of trade union premiums and/or to register the status of a protected employee.

Lastly, it is worth noting that an employee’s National Registry Number (Social Security Number) may only be processed for the purpose of complying or proceeding with ONSS (National Social Security Office) requests and/or filings, and in no case as a company internal reference for the employee.

Non sensitive Personal Data may be processed by a Data Controller in the circumstances mentioned in Section 4(e) above and, in particular, for the performance of a contract to which the Data Subject is a party, for the purpose of carrying out the Data Controller’s legal obligations, or where processing is
necessary for the purposes of the legitimate interests of the Data Controller not overriding the Data Subject’s fundamental rights and freedoms.

A fallback justification for processing non sensitive Personal Data in the employment context may be the Data Subject’s consent. However, employees may not consent to the processing of their sensitive Personal Data (except where the processing aims to grant advantages to the employee), and there is some concern whether employees may validly consent to the processing of their Personal Data by their employers (see Section 5(d) below).

5. Consent

a. General

Consent of the Data Subject is generally a straightforward way to justify the collection, processing and disclosure of Personal Data. Consent given by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances.

Consent is contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to only cover the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

There is no mandatory requirement that consent be in writing, except for the processing of sensitive Personal Data. It may be provided orally or in different forms and formats. In addition, the Data Subject also has the right to withdraw consent at any time.

There is no specific language requirement other than resulting from Belgium’s general linguistic legislation, which requires the use of a specific language depending on the geographical location of the employer and the status of the employee. The Data Subject should in any case be informed about the processing of his/her Personal Data (and be invited to give his or her consent, as the case may arise) in an understandable language.

b. Sensitive Data

Belgian law recognizes sensitive Personal Data as a special category of Personal Data. It is subject to additional and special consent requirements. While sensitive Personal Data may only be collected and processed with the express (written) consent of the Data Subject, it may be processed without obtaining consent in certain prescribed circumstances.
c. Minors

The general rule is that minors under the age of 18 are considered incapable of giving consent. However, parents or legal guardians of minors are allowed to provide consent on behalf of the minor, and may even be allowed to obtain information about the minor from third parties without the need of consent from the minor. Further, parents or legal guardians have the right to be informed of the collection of information, to access and rectify the Personal Data and to have recourse to the Privacy Commission or the President of the First Instance Court. Nevertheless, there are certain circumstances where consent given by a minor may be considered valid. In its Opinion 38/2002 relating to the privacy protection of minors on the Internet, the Privacy Commission seems to consider that the legal representative’s consent should not be systematically required when data relating to minors who have not reached the age of discernment (which is between 12 and 14 years old) is processed on the internet.

d. Employee Consent

The Article 29 Working Party has produced an opinion on the processing of Personal Data in the employment context which states that it is not appropriate for an employer to try to rely on an employee’s consent as it is unlikely to be freely given.

In Belgium, the processing of sensitive Personal Data generally cannot be validly authorized by employees, except where the processing aims to grant them advantages.

However, subject to caution, such consent might validly permit the processing of non-sensitive Personal Data.

However, employee consent is generally not required where the data processing is necessary to carry out an employment contract or administer an employment relationship, or to fulfill a legitimate interest of the employer.

e. Online/Electronic Consent

In Belgium, online or electronic consent is permissible and deemed effective if properly structured and evidenced.

However, where the law requires written consent (e.g., regarding sensitive data), specific requirements need to be met.

6. Notice Requirements

A Data Controller that collects Personal Data must provide Data Subjects, at the time his or her data is collected or first recorded, with information about the Data Controller’s identity and address; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; whether the provision of
Personal Data is mandatory and the consequences of refusal to provide Personal Data; the rights of access, rectification and objections of the Data Subject; where the Personal Data is to be transferred; where the Personal Data is to be stored; and how to access and/or correct the Data Subject’s Personal Data.

7. Processing Rules

A Data Controller that processes Personal Data must: limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; anonymize the Personal Data whenever possible; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

In addition, when entrusting the processing of Personal Data to a third party processor acting on its behalf (a “Data Processor”), the Data Controller must choose a Data Processor providing sufficient guarantees in respect of the technical and organizational measures governing the processing to be carried out.

In addition, the processing must be carried out under a contract that (i) is in writing, (ii) requires the Data Processor to act - and causes any person acting under its authority and having access to personal data to act - only on the instructions of the Data Controller, (iii) requires the Data Processor to comply with security obligations equivalent to those imposed on the Data Controller, and (iv) lays out the liability of the Data Processor towards the Data Controller.

8. Rights of Individuals

Data Subjects have the general right to: be informed by a Data Controller of the Personal Data the Data Controller holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; object to the processing of Data Subject’s Personal Data for direct marketing purposes at any time and free of charge; and request the deletion and/or destruction of the Data Subject’s Personal Data for legitimate reasons.

9. Registration/Notification Requirements

Any Data Controller established in Belgium or, if established outside the European Economic Area, using means located on the Belgian territory for the purpose of its data processing (other than for mere transit purposes) is required to file a notification with the Belgian Privacy Commission before any wholly or partly automated data processing starts. Exemptions to the requirement for notification apply for the processing of data dealing merely with the management of employees’ wages and/or payroll, as well as for mere clientele management, subject to certain conditions.
10. Data Protection Officers
In Belgium, there is no requirement to appoint or designate a data privacy officer accountable for the privacy practices of the organization.

11. International Data Transfers
Except for the communication of health-related data (see Section 4(e)), transfers of Personal Data from Belgium to EEA Member States are permitted without the need for further approval. The same applies to transfers to countries that have been recognized by the European Commission as having adequate data protection laws. Subject to the specific exceptional authorizations above, Personal Data may not be transferred to countries outside the EEA, unless the destination country provides adequate protection for the Personal Data. Exceptions are as follows:

- the Data Subject has given his or her unambiguous consent to the transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or for the implementation of pre-contractual measures taken in response to the request of the Data Subject;
- the transfer is necessary for the performance of a contract concluded or to be concluded in the interest of the Data Subject between the Data Controller and a third party;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;
- the transfer is made from a public register which, by law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest; or
- a data transfer agreement is in place. Following a Protocol entered into between the Privacy Commission and the Belgian Department of Justice in June 2013, as amended in 2014, all data transfer agreements intended to cover transfers of data out of the European Economic Area to countries not providing an adequate level of data protection must be submitted to the Belgian Privacy Commission. Data transfers agreements not conforming to EU Commission’s Standard Contractual Clauses must be approved by the King (i.e., the Federal Government).

12. Security Requirements
Data Controllers and Data Processors are required to take steps to: ensure that Personal Data in their possession and control are protected from unauthorized access and use; implement appropriate physical, technical and
organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Data Controllers that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. In case of an occurrence of data breach, the outsourcing organization may be held liable together with the third party provider.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints; data authority investigations/audits; seizure of equipment or data; civil actions; criminal proceedings; and/or private rights of action.

The court may also order the seizure of any privacy infringing equipment or data, the rectification or destruction of Personal Data, and the publication of its judgment in whole or by excerpt in one or more newspapers. The court may also prohibit the Data Controller from processing any personal data for up to 2 years.

15. Data Security Breach

There is currently no express general legal requirement under Belgian law for a Data Controller or a Data Processor to notify Data Subjects or government authorities about the hacking of Personal Data or, more generally, to notify them about a security failure allowing unauthorized access to such data.

However, the Act of 10 July 2012 amending the 2005 Electronic Communications Act implemented into Belgian law a limited notification obligation in case of a security breach of an electronic communications service accessible to the public relating to Personal Data. In case of a security breach of an electronic communications service accessible to the public relating to Personal Data, the undertaking providing the services must notify without delay the Belgian Institute for Post and Telecommunications (BIPT) about the data breach. Where such breach may negatively affect Personal Data or a subscriber or an individual’s privacy, the undertaking must also inform without delay the subscriber or individual at stake about the breach.

The notification to the subscriber or individual is not necessary if the undertaking has satisfactorily evidenced to the BIPT that it put all appropriate technological measures in place and that these were applied to data concerned by such breach. Such technological measures render data incomprehensible for any person not authorized to access them. Without prejudice to the foregoing, the BIPT may require that the undertaking inform the concerned subscribers or individuals.
The notification to be made to the subscriber or individual shall describe, at minimum, the nature of the Personal Data breach and contact points where further information may be obtained, and recommend measures to be taken to reduce potential negative consequences. In addition, the notification to the BIPT must describe the consequences of the data breach, the appropriate measures proposed or implemented to remedy the breach.

Additionally, the Belgian Act of 11 March 2003 on certain legal aspects of the information society, makes it an obligation for transport, caching and hosting service providers to report to the public prosecutor alleged illegal activities on their systems of which they become aware. This might then apply to the hacking of Personal Data or to the unauthorized access to data they transport, cache or host.

More generally, informing the Data Subjects about a potential data security breach arguably falls within the scope of the Data Controller’s general loyalty obligation set forth by Article 4 of the DPA, combined with the obligation to inform data subjects about the “recipient(s)” of their data (Article 9 of the of the DPA).

In a Recommendation nr. 1/2013, dated January 21, 2013 on information security and, in particular, working with computer files, the Belgian Privacy Commission even considers that companies must implement procedures for reporting data security incidents. In the case of a public incident (it being noted that a public incident is not defined by the Privacy Commission), the Privacy Commission considers that it should be informed of the cause(s) and impact of the incident with 48 hours and that awareness campaigns to inform the public should be initiated within 24 to 48 hours following notification to the Commission.

In any case, in accordance with the Belgian civil law principles of good faith and fairness in contractual relationships between the parties as well as with the Belgian law on torts, it is advisable for a Data Controller to inform Data Subjects about a potential data security breach so that the latter can take appropriate measures, if any, to mitigate their risks or prejudice.

Any Data Controller that is involved in a data breach situation may be subject to the sanctions outlined under Section 14 above.

Violations of the limited security breach notification requirement under the 2005 Electronic Communications Act are also sanctioned by fines from € 300 to € 300,000.

16. Accountability

Subject to regulatory guidance, organizations in Belgium may be required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.
17. Whistle-blower hotline

Whistle-blower hotlines may be established in Belgium provided they are in compliance with local laws and with requirements of registering and filing with the Belgian Privacy Commission. (cf. the Belgian Privacy Commission’s recommendation of 2006 regarding the compatibility of whistleblowing hotlines with the Belgian DPA).

18. E-discovery

When implementing an e-discovery system, an organization must comply with the general requirements of the DPA, as well as with other legal requirements applicable to the review of employees’ or Data Subject’ electronic communication data, including, the Criminal Code, the Electronic Communications Act of 13 June 2005, and the Collective Bargaining Agreement n° 81 on the monitoring of electronic online communication data. The organization may be required to obtain the consent of employees. In addition, an organization is required to advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information in accordance with the above-mentioned legal texts.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization will have to comply with the general requirements of the DPA. Besides, to the extent that a spam-filtering solution consists of intercepting e-mails, it must comply with the Electronic Communications Act of 13 June 2005 and the Criminal Code. Article 125, § 1, 6°, of the Electronic Communications Act provides that Article 124 of the same and Articles 259bis and 314bis of the Criminal Code (which prohibit the interception of data transferred by way of telecommunications without the consent of all persons interested, directly or indirectly, in such communications) do not apply to acts carried out for the sole purpose of providing spam-filtering services to the end-user, provided that the end-user’s prior authorization is obtained to that effect.

20. Cookies

There are specific laws/rules that regulate the deployment of cookies, and hence, the use of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used, except in limited exemptions. The Belgian Privacy Commission issued guidance on the use of cookies and similar technologies in February 2015.
21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, depending on the communication means to be used. Consent can generally not be inferred from a Data Subject’s failure to respond. An organization may be required to obtain consent for a specific activity. The Belgian Privacy Commission issued guidance on the use of personal data for direct marketing purposes in 2013.
Brazil

Esther Flesch
Sao Paulo
Tel: +55 11 3048 6940
esther.flesch@bakermckenzie.com

Bruno Maeda
Sao Paulo
Tel: +55 11 3048 6838
bruno.maeda@bakermckenzie.com

Flavia Rebello
Sao Paulo
Tel: +55 11 3048 6851
flavia.rebello@bakermckenzie.com
1. Recent Privacy Developments

At the beginning of 2015, the Brazilian Ministry of Justice submitted for public consultation a first Draft Bill of Law for Protection of Personal Data (the “Draft Bill”). The Draft Bill applies to individuals and public and private entities that process Personal Data through automated means, and aims to regulate the treatment and protection to be given to Personal Data in Brazil in view of the Data Subject’s fundamental rights to freedom, intimacy and privacy. As drafted, the Bill of Law intends to create a set of obligations and responsibilities to all public and private entities and individuals who collect and use Personal Data in any way, regardless of where such entity is located or where the data is to be stored.

The key provisions contained in the Draft Bill include the requirement to obtain consent from the Data Subject to process Personal Data, subject to limited exceptions (for instance, no consent is needed in cases where data collected was previously made public or if data has been unrestricted); and the prohibition to process Sensitive Personal Data, subject to certain limited exceptions. For instance, a Data Subject needs to provide separate consent to allow the processing of Sensitive Data, and must be given the right to revoke the consent at any time. It also expressly forbids the processing of Sensitive Personal Data revealing racial, genetic and sexual information, as well as religious, moral and political convictions.

In addition, the Draft Bill provides that minors aged 12 to 18 may be permitted to provide consent for processing of their Personal Data, subject to certain conditions (which consent may be revoked at any time by the parents or legal representatives of the minor). The treatment of Personal Data of children below 12 years old will, however, require parental authorization.

In several instances, the Draft Bill also suggests that a specific governmental agency is to be created to regulate this matter and verify compliance with the law. This fact is also sustained by declarations of those agents of the Ministry of Justice more closely involved with the Draft Bill.

It is unclear whether the Draft Bill will be modified by the Ministry of Justice based on the comments that it received during the public consultation process, and it is difficult to predict how it will evolve during the legislative process at the National Congress.

2. Emerging Privacy Issues and Trends

Besides the discussion raised by the Draft Bill, as discussed in Section 1, consumer authorities in Brazil have been consistently enforcing privacy rules related to consumer relations. Enforcement actions range from requests for explanation from entities to administrative procedures that can lead to the imposition of penalties on entities deemed not to be in compliance with privacy rules within the Consumer Defense Code.
3. Law Applicable

The legal protection afforded to Personal Data arises from general rules and principles disseminated in several different pieces of legislation.

**Brazilian Federal Constitution** (Article 5, X): contains general provisions on privacy. According to the Brazilian Federal Constitution, the individual’s rights to intimacy, privacy, honor and image are fundamental rights and any violation thereof entitles the Data Subject to indemnification for both moral and material damages. Moreover, the secrecy of correspondence, telegraphic, data and telephone communication is also a Constitutional guarantee.

**Brazilian Civil Code** (Law No. 10,406/02, Article 21): among other general provisions, it considers the right to privacy as a personality right, which cannot be waived or assigned as a matter of public policy.

**Brazilian Consumer Protection Code** – CDC (Law No, 8078/90): contains certain rules regarding the collection, storage and use of consumer databases. The CDC regulates the creation of databases containing consumers’ personal information. Pursuant to the CDC, “consumer” is any individual or legal entity that acquires a good or a service as an end-user. By this definition of consumer, the CDC governs not only retail sales to consumers, but also sales of products and services to legal entities, that will be treated as consumers when and if they are end-users of products and services (on a case-by-case basis).

**Internet Legal Framework** (Law No. 12,965/14): establishes general principles, warranties, rights and duties that govern the use of the Internet in Brazil and regulates the protection of privacy and data online. It contains several provisions regarding Internet users’ rights to the protection of logs, Personal Data and private communications, as pointed out in later sections in this chapter. Although the Internet Legal Framework is very recent and, in theory, only applies to data collected over the Internet, it may be, henceforth, used by courts as a general guideline in the absence of a specific data privacy law.

Some aspects of this Law are still to be regulated by a governmental decree not yet enacted until this date, but a draft decree had been under public consultation at the beginning of 2015.

**Brazilian Criminal Code**: as amended by Law No. 12,737/12, has general provisions addressing crimes relating to the inviolability of correspondence and crimes of invasion of information technology device. Accordingly, the Law provides that it is a criminal offense to invade third parties’ information devices, whether or not such devices are connected to the Internet, by means aimed at obtaining, altering or destroying data or information without express or implied authorization from the device owner or to install vulnerabilities to obtain illicit advantages. The crime is punishable by detention of three (3) months to one (1) year, plus payment of a fine. This penalty also applies to
anyone who makes, offers, distributes, sells or discloses a computer device or software aimed at enabling the conducts described above. Also, in the event that the invasion results in obtaining content from private electronic communications, industrial or trade secrets, confidential information or the unauthorized remote control of the device, the penalty is increased to imprisonment of six (6) months to two (2) years, plus payment of a penalty. This latter penalty is also increased in the event that the data or information obtained is disclosed, traded or transmitted to third parties.

**Federal Law 9,296/96 - Interception of telephone communication Law:** determines that such procedure may only be authorized by a judge in the context of a criminal investigation.

**Complementary Law No. 105/01:** establishes rules regarding bank secrecy with which financial institutions must comply in the banking sector. Please note that other sector-specific rules may also apply.

**Brazilian Information Access Law (Law No. 12,527/11, article 4, IV):** regulates the access to information held by public entities and agencies in Brazil; it also gives a legal definition of what is considered “Personal Data”, as analyzed in Section 4.

4. Key Privacy Concepts

a. **Personal Data**

Brazilian laws do not contain a specific definition of “Personal Data”. Nevertheless, the Constitutional protection of privacy and the provisions of the Civil Code are very broad as they refer to the protection of the individual’s privacy and intimacy. The Consumer Protection Code refers to any information included in registrations or forms and any data regarding the acquisition of products or services.

In addition to the above, Brazilian Information Access Law defines personal information as information regarding an identified or identifiable individual (i.e., subject to be identified). This definition may be used as reference for purposes of data protection laws and is generally adopted in courts and by scholars when addressing this matter.

b. **Data Processing**

There is no definition of “Data Processing” under Brazilian laws. In the absence of a specific definition and due to the Constitutional protection of privacy, the concept of data processing should be understood in a broad way, including any form of use, collection, processing, disclosure, transfer, organizing, amending, recording, handling and storage of data, whether on a manual or automated basis.

c. **Processing by Data Controllers**

Brazilian laws do not contain specific definitions of “Data Controllers”.

64  Baker & McKenzie
d. Jurisdiction/Territoriality

The Brazilian Federal Constitution, Civil Code, and Consumer Protection Code are considered public order rules and will apply to the use, collection, processing, disclosure, transfer, organizing, amending, recording, handling and storage of data relating to Data Subjects residing in Brazil.

The Internet Legal Framework sets forth the mandatory application of Brazilian laws for the collection, storage and processing of Personal Data or communications if: (a) at least one of such actions takes place in Brazil or (b) at least one of the endpoints is located in Brazil. This rule shall equally apply to foreign companies (i) to the extent there is a Brazilian entity of the corporate group in Brazil or (ii) their services are offered to the Brazilian public. The main goal of such provisions is to prevent Brazilian entities of multinational groups from arguing that data is stored in servers abroad, subject to foreign laws and, accordingly, that Brazilian laws should not apply.

e. Sensitive Personal Data

There is no specific definition of “Sensitive Personal Data” under Brazilian laws.

f. Employee Personal Data

There is no specific definition of “Employee Personal Data”. Consequently, employee’s Personal Data is generally treated as other Personal Data, but with some particularities that are typical of an employment relationship (please refer to Section 5(d) below).

5. Consent

a. General

Consent of the Data Subject is required prior to the collection, use, processing, transfer and disclosure of Personal Data. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances. The consent should include: (a) clear and complete information on the purposes for which the company intends to collect information; (b) to whom data may be disclosed; (c) where data will be stored (indicating if cross-border transfers are necessary/envisaged) and; (d) what means are used to protect it.

When the Data Subject gives consent, it only covers the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

The Data Subject also has the right to withdraw consent at any time in given circumstances.
b. Sensitive Data

There are no specific rules in Brazil defining or regulating Sensitive Personal Data. It is important to note that the more sensitive the data is, the greater the risks of claims for damages regarding its improper collection, use or disclosure. Therefore, to the extent feasible, any use, including without limitation, the collection and processing of Sensitive Personal Data (e.g., health information) without the previous and specific consent from the Data Subject should be avoided.

c. Minors

According to the Brazilian Civil Code, only individuals over the age of 18 are capable of binding themselves personally. Minors under 16 are considered absolutely incapable, while those between 16 and 18 are considered relatively incapable (in other words, they can bind themselves with the assistance of their parents or guardians). As the collection of Personal Data in Brazil (under the Federal Constitution and the Civil Code) depends on the prior consent of the Data Subject, parental consent is required for those under 18 years old.

It should be noted, however, that relatively incapable minors (between 16 and 18) will not be able to claim the invalidity of a contract (or the consent to collect, process and/or use Personal Data) if they have falsely declared themselves to be above 18.

d. Employee Consent

There are no specific rules addressing this issue. Consequently, Personal Data relating to an employee is generally treated in the same way as other Personal Data. It should be noted, however, that the general interpretation of Brazilian laws is that, with respect to employee Personal Data, the Constitutional privacy rights should be interpreted in a more flexible manner in view of the rights granted by the Brazilian Labor Code to employers to manage and control their employees’ activities during working hours, as well as by the Brazilian Civil Code, which in its Article 932, III, establishes that the employer can also be liable for the implications arising from actions taken by its employees during working time. In fact, based on those grounds, Brazilian Courts have adopted the understanding that the employer has the right to monitor and review the use of the electronic resources (including email, Internet and corporate computers) made available to the employees, regardless of previous notice, as long as the employee is advised of such possibility and has, therefore, no privacy expectations when using these work tools.

e. Online/Electronic Consent

There is no provision that specifically addresses online/electronic consent requirements. However, considering that the Internet Legal Framework applies to data collected over the Internet and requires the Data Subjects’ prior express consent, it is implied that online/electronic consent is permitted.
Since the Data Subject’s consent shall be express, an opt-in system (e.g., a check-box or an “I agree” button) is usually understood as the appropriate means for such purpose.

Electronic consent mechanisms are generally enforceable in Brazil and considered sufficient to evidence the Data Subject’s agreement with the terms of a consent form to the extent that the Data Controller is able to prove that the systems and processes used to secure the consent are robust and reliable for the purposes of establishing the authenticity and integrity of the consent.

It is worth noting that under the Internet Legal Framework, consent language shall be visually different from other dispositions of the agreement, such as the terms of use. The law does not establish a clear definition of how different such language should be, but such obligation is commonly interpreted as language which should stand out from the other provisions, by using bold or capital letters, or a different font size, for instance. Furthermore, consumer protection rules further provide that the terms of the agreement must be readable (with a minimum font size of 12 pt.) and written in easily comprehensible Portuguese.

6. Information/Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: (a) the organization’s identity; (b) the types of Personal Data being collected; the purposes for collecting Personal Data; (c) its privacy practices (which must be given in a clear and transparent way); (d) third parties to which the organization will disclose the Personal Data; (e) the consequences of not providing consent; (f) the rights of the Data Subject; (g) how the Personal Data is to be retained; (h) where the Personal Data is to be transferred; (i) where the Personal Data is to be stored; (j) how to access and/or correct the Data Subject’s Personal Data; and (h) the duration of the proposed processing.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymous Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: (a) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; (b) access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; (c) request the correction of the Data Subject’s Personal Data; (d) request the deletion and/or
destruction of the Data Subject’s Personal Data; and (e) exercise the writ of habeas data.

9. Registration/Notification Requirements
There are no requirements for organizations that collect and process Personal Data to register, file or notify a local data authority.

10. Data Protection Officers
There is no requirement for organizations to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers
The Internet Legal Framework determines that Personal Data may only be transferred to third parties (including abroad) upon the free, express and informed consent of the Data Subject.

12. Security Requirements
Organizations are required to take steps to: (a) ensure that Personal Data in its possession and control are protected from unauthorized access and use; (b) implement appropriate physical, technical and organization security safeguards to protect Personal Data; and (c) ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

The Internet Legal Framework determines that security measures and proceedings shall be informed to the Data Subject in a clear manner and shall meet the standards determined by the applicable regulation. However, such regulation is yet to be issued under a governmental decree, which had been under public consultation in early 2015.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and are required to comply with sector specific requirements. Organizations shall be liable together with third party providers in case of breach by the latter.

The Internet Legal Framework determines that Personal Data may only be transferred to third parties (including abroad) upon the free, express and informed consent of the Data Subject.
14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, administrative fines, penalties, or sanctions, civil actions, and/or criminal proceedings.

Specifically in relation to the Internet Legal Framework, failure to comply with any of its rules regarding protection of Personal Data and private communications may result in (i) warnings; (ii) fines in the amount of up to 10% of the economic group's gross revenues in Brazil in the last fiscal year; (iii) temporary suspension of data collection activities in Brazil and/or (iv) prohibition of data collection activities in Brazil. Furthermore, the law expressly determines that the Brazilian entity of a group shall be jointly liable with the foreign entity for any fines imposed on the

15. Data Security Breach

There are no specific rules addressing data security breaches. However, as Data Controllers are generally liable for any data security breach, it is highly advisable to inform the affected Data Subjects and the relevant bodies as soon as the Data Controller becomes aware of a data security breach.

This is especially important in situations where an early notice can be helpful to mitigate possible damages to the Data Subjects (e.g., by allowing the Data Subjects to change passwords or take other precautionary measures to avoid damages). Accordingly, the Data Controllers may also be able to reduce their liability for damages that can be mitigated by means of an early notification of the security breach.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions and/or class actions. However, neither the Internet Legal Framework nor any other Brazilian law regulates the applicable procedure for such cases.

16. Accountability

Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Brazil as long as they are in compliance with local laws.

18. E-Discovery

In Brazil, there are no specific rules regarding the discovery of electronically stored information, therefore, the general rules under the Brazilian Civil Procedure Code shall apply.
Moreover, if an organization obtains prior written consent from its employees for the collection of Personal Data in connection with the implementation of an e-discovery system, then no specific issues should arise. On the other hand, if no consent is obtained, specific privacy issues may develop depending on the specific circumstances of the case and the type of data to be collected, processed and/or disclosed.

19. Anti-Spam Filtering

In principle, no privacy issue arises from the introduction of a spam-filtering solution in an organization. However, in case there is a possibility of the organization gaining access to private emails received by an employee due to the spam-filtering solution, the employee should be previously informed of such possibility so that he or she would have no privacy expectations related to the use of the corporate email account.

20. Cookies

There are no specific laws/rules in Brazil that regulate the use and deployment of cookies. Nevertheless, in view of Brazilian general data privacy laws, to the extent that any information collected through cookies identifies or might personally identify a Data Subject, prior express consent (opt-in) should be secured from the Data Subject for such data collection, use, storage, process and transfer.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.

- **Do-Not-Call Registry** - The State of São Paulo Decree No. 53,921, of December 30, 2008, created the Telemarketing Enrollment List to Blocked Calls (“Register”), regulating State Law No. 13,226 of December 07, 2008. This legislation benefits users of fixed and mobile telephony with area code numbers from the State of São Paulo. The Consumer Defense and Protection Foundation (“PROCON”) is responsible for the maintenance and implementation of the Register, which is available through the Internet or in local service centers of the State of São Paulo. Thirty days after consumers are listed in the Register, telemarketing companies will no longer be allowed to call the numbers included, unless the consumer grants prior permission in writing and with an express expiration date. Companies that fail to comply with the rules of State Decree No. 53,921 will be subject to administrative penalties of the Consumer Protection Code. Philanthropic entities that use telemarketing to raise funds are exempted from the effects of the Decree. Moreover, many States in Brazil have adopted similar laws such as Alagoas (Law No. 7,127/09), Amazonas (Law No. 3,633/11), Ceará (Law 15.111/12),
Espírito Santo (Law No. 9,176/09), the Federal District (Law No. 4,171/08), Goiás (Law No. 17,424/11), Maranhão (Law No. 9,053/09), Mato Grosso do Sul (Law No. 3,641/09), Paraíba (Law No. 8,841/09), Paraná (Law No. 16,135/09), Pernambuco (Law No. 13,796/09), Rio Grande do Sul (Law No. 13,249/09), and Santa Catarina (Law No. 15,329/10).

**Marketing Emails** - A Code of Self-Regulation (“Code”) aimed at the responsible, ethical and correct use of marketing emails, and which serves as guidance for the use of email for marketing purposes, has been published by a Council formed by representatives of 14 civil society organizations. Some of these associations are the Brazilian Direct Marketing Association, the Brazilian Internet Steering Committee, the Brazilian Internet Providers Association, and the Brazilian Consumer Defense Association (“PRO TESTE”). While the Code is not a formal law, it provides important guidelines on how marketing emails can be sent without breaching Brazilian privacy law. In addition to other provisions, the Code requires the parties to provide a “Privacy and Data Use Policy” on their respective websites, under penalty of, among others, recommendation of blockage of the sender’s domain name. The Code adopted an “opt-in” system according to which non-requested messages are prohibited. The only exception to this is when the parties have a long standing commercial relationship which implies the concept of the so called “soft-opt-in”. The Code also contains other requirements that must be observed, including the clear identification of the sender, the subject of the e-mail must relate to the content of the e-mail and an opt-out mechanism should be offered to the recipient in the body of the message. Such opt-out option shall include (i) one unsubscribe link, and (ii) at least one additional contact option for such purpose (e.g., e-mail, telephone, SMS, mail, etc.). In addition, the Code provides that the users’ option to unsubscribe must be complied with within two days when directly requested by the user through an unsubscribe link, or within five days when requested by other means. Furthermore, the company responsible for sending marketing emails must use its own domain names. In case of violation of any of the Code’s provisions, sanctions shall be imposed by an Ethics Committee formed by the Self-Regulation Code Council.
Canada

Lisa Douglas
Toronto
Tel: +416 865 6972
lisa.douglas@bakermckenzie.com

Arlan Gates
Toronto
Tel: +416 865 6978
arlan.gates@bakermckenzie.com

Theodore Ling
Toronto
Tel: +416 865 6954
theodore.ling@bakermckenzie.com

Jonathan Tam
Toronto
Tel: +416 865 2324
jonathan.tam@bakermckenzie.com

Eva Warden
Toronto
Tel: +416 865 2350
eva.warden@bakermckenzie.com
1. Recent Privacy Developments

Amendments to Personal Information Protection and Electronic Documents Act

In June 2015, amendments to the Personal Information Protection and Electronic Documents Act ("PIPEDA") came into effect. PIPEDA generally governs the collection, use, and disclosure of personal information by private sector organizations in all Canadian provinces except for Alberta, British Columbia, and Québec. Some of the key changes to PIPEDA are as follows.

- Organizations are now expressly permitted to use and disclose individuals’ personal information without their knowledge or consent where the personal information is necessary to determine whether to proceed with or complete a business transaction, and certain measures are taken to protect the information. If the transaction is not completed, all personal information must be returned or destroyed by the recipient. If the transaction is completed, the recipient may continue to use the personal information as long as certain security measures are taken, the personal information is necessary for carrying on the activity that was the object of the transaction, and the individuals are notified of the completion of the transaction and the disclosure of their personal information within a reasonable amount of time afterwards. Notably, this exception to the general consent requirement does not apply where the purpose of the transaction is to buy, sell, or lease personal information.

- Federal works, undertakings, or businesses (“FWUBs”) may now collect, use, and disclose the personal information of an individual without his or her consent where it is necessary to establish, maintain, or terminate an employment relation between that individual and the FWUB, and the FWUB has informed the individual of the purpose of the collection, use, and disclosure of the information.

- On an unspecified day in the future, amendments regarding data breach notifications will come into force. These amendments require organizations affected by a data breach to make prescribed disclosures to the Office of the Privacy Commissioner of Canada (the “OPC”) and affected individuals where there is a reasonable expectation that the data breach could create a risk of significant harm. Knowingly failing to report a data breach could result in fines of up to C$100,000 as well as publication of any such data breach.

- Organizations may now disclose personal information to another organization without the knowledge or consent of an individual where it is reasonable for the purposes of investigating a breach or possible breach of an agreement or Canadian law and it is reasonable to expect that obtaining the individual’s consent would compromise the investigation. Similar exceptions also apply to investigations involving the detection,
suppression or prevention of fraud where a person is suspected of being a victim of financial abuse.

- The amendments authorize the OPC to enter into binding compliance agreements with organizations where it believes on reasonable grounds that an organization has, will, or is likely to commit an act or omission that would contravene PIPEDA. Compliance agreements are voluntary on the part of the organizations and, in exchange, the OPC will not apply to the court for a hearing or suspension of any pending applications. At the same time, entering into a compliance agreement does not preclude individual complaints against the organization or the prosecution of an offense under PIPEDA. The agreements may contain any terms that the OPC considers necessary to ensure compliance with PIPEDA. If the OPC is of the opinion that the agreement has been complied with by the organization, the OPC shall notify the organization and withdraw any outstanding applications. If, however, the OPC is of the opinion that the agreement has not been complied with by the organization, the OPC shall notify the organization and may apply to the court for an order requiring compliance with the agreement or commence or reinstate proceedings under PIPEDA.

**Canada’s Anti-Spam Law Provisions on Installing Computer Programs Now in Force**

On January 15, 2015, the provisions of Canada’s Anti-Spam Law (“CASL”) that apply to the installation of computer programs came into force. These provisions are separate from those under CASL that prohibit the transmission of commercial electronic messages without the recipient’s consent, which came into force last year. The provisions on the installation of computer programs under CASL generally prohibit the installation of a program on another person’s computer system in the course of a commercial activity without obtaining the express consent of the owner or authorized user of that computer system in a prescribed manner. Specific types of computer programs such as cookies and HTML code are exempt from this prohibition where it is reasonable to believe that the owner or authorized user of the computer system consents to that program’s installation. The term “computer system” generally covers laptops, desktops, mobile devices, gaming consoles, and other connected devices.

To obtain a person’s express consent to install a computer program on their computer system, an organization must at the time of installation disclose certain contact information, provide a clear and simple description of the function and purpose of the program to be installed, and state that the person can withdraw their consent. Where a person expressly consented to the installation of an update or upgrade of a computer program at the time the program was installed, an organization may generally install such updates or
upgrades on that person’s computer without having to obtain their fresh express consent.

Special requirements may apply if an organization installs a program (including an update or upgrade) on another person’s computer system which causes it to operate in a manner contrary to the reasonable expectations of its owner or authorized user. These special requirements, which are more onerous and intended to deter unauthorized installation of malware, apply to programs that perform any of a prescribed list of functions, such as interfering with the user or authorized user’s control of the computer system, or causing the computer system to communicate with another computer system without the authorization of the owner or authorized user.

As with the provisions relating to the sending of commercial electronic messages, penalties for non-compliance run as high as CAD $10 million in potential administrative penalties for organizations. Starting on July 1, 2017, a private right of action for non-compliance with CASL will also become available, exposing organizations to the risk of class actions. Parties found to have installed programs in contravention of CASL could be subject to statutory damages of CAD $1 million per day on which a contravention occurred, in addition to compensatory damages.

Several Enforcement Actions Taken under Canada’s Anti-Spam Law

The maximum penalty for a violation under Canada’s Anti-Spam Law (“CASL”) is C$10 million for organizations. In early March 2015, the Canadian Radio-television and Telecommunications Commission (the “CRTC”), which regulates the anti-spam provisions under CASL, announced that it would seek a C$1.1 million penalty against a Québec-based company for violating CASL. According to the CRTC, the infringing company sent commercial emails to recipients without their consent and failed to include proper unsubscribe mechanisms in the messages.

In addition, the CRTC announced in late March 2015 that it had entered into an undertaking with an organization that runs a popular dating service for C$48,000 after investigating consumer complaints that the company sent commercial emails to registered users without an unsubscribe mechanism that could be readily performed. In July 2015, a Canadian airline also agreed to pay C$150,000 as part of an undertaking with the CRTC. The CRTC alleged that the airline failed to include or clearly set out an unsubscribe mechanism in commercial emails, failed to provide complete contact information on commercial emails, failed to honour unsubscribe requests within ten business days, and was unable to provide proof that it had obtained consent for each electronic address that received its commercial emails. In addition to the payment, the airline has undertaken to implement an enhanced compliance program that will include increased training and education for staff and improved corporate polices and procedures.
Canada’s Top Court Releases Two Decisions on the Role of Privacy in State Investigations

The Supreme Court of Canada (“SCC”) released two decisions that contribute to the growing Canadian case law on individual privacy interests in the context of the state’s exercise of its investigative powers and subsequent use of evidence. In *R v Fearon*, 2014 SCC 77, the police conducted a warrantless search of the accused’s cell phone in connection with a robbery before they had located the stolen items or the weapon used in the robbery. The evidence discovered in the course of the search, which included a draft text message and a photograph of the handgun used in the crime, was used to convict the accused at trial. In considering the constitutionality of the search of the cell phone, the SCC established that the following four conditions must be met for the search of a cell phone or similar device incidental to arrest to comply with the Canadian Charter of Rights and Freedoms:

1. The arrest must be lawful.
2. The search must be “truly incidental” to the arrest, meaning searches must be done promptly upon arrest in order to effectively serve law enforcement purposes. Specifically, these purposes may include protecting the police, the accused or the public; preserving evidence; and discovering evidence if there is a risk that the investigation will be stymied or significantly hampered absent the ability to conduct the search.
3. The nature and the extent of the search must be tailored to its purpose, meaning that, in practice, only recently sent or drafted emails, texts, photos and the call log will generally be available.
4. The police must take detailed notes of what they have examined on the device and how they examined it.

In this case, the SCC held that the search breached the accused’s constitutional right to security against unreasonable search and seizure because it did not meet the fourth condition above. Nonetheless, the SCC did not exclude the evidence because the impact on the accused’s protected interests was not especially grave in this case. Moreover, other factors (such as society’s general interest in the adjudication of the case on its merits) favoured inclusion.

Separately, in *Imperial Oil v Jacques*, 2014 SCC 66, plaintiffs at the exploratory stage of a Quebec-based civil class action were allowed to access wiretap evidence gathered in a related Competition Bureau criminal investigation. The SCC confirmed that disclosure of the evidence to the plaintiffs was permitted subject to two conditions: that the recordings be disclosed solely to the lawyers and experts participating in the civil proceedings, and that they be screened to protect the privacy of third parties having nothing to do with the proceedings.
However, in an acknowledgment of the privacy protections enshrined in the **Criminal Code of Canada** and Quebec **Charter of Human Rights and Freedoms**, the SCC held that there is no right to access intercepted communications until those interceptions have been found, or are conceded to be, lawful and admitted into evidence in a criminal proceeding. Moreover, the SCC cautioned that while a trial judge has discretion to order disclosure under the Quebec **Code of Civil Procedure**, such a request must be denied where either legislation or the courts have established an immunity from disclosure. According to the SCC, the judge's exercise of discretion in determining whether and how to order disclosure may take into account a number of considerations, such as: the relevance of the documents to the issues between the parties (which generally is interpreted broadly at the exploratory stage), the potential impact of disclosure on the privacy interests of a party or third party to the proceedings, the efficient conduct of criminal proceedings, and the accused's right to a fair trial.

The results of these cases suggest a tendency towards permitting disclosure and use of information obtained in the course of criminal investigations.

**Federal Court Certifies Class-Action lawsuit for Tort of Intrusion upon Seclusion**

The Federal Court of Appeal’s decision in *Condon v The Queen*, released in July 2015, has major implications for organizations that have experienced large-scale data breaches. In *Condon v The Queen*, the Federal Court of Appeal upheld the decision of the Federal Court to certify a class action lawsuit based on the tort of intrusion upon seclusion. In this case, over 500,000 Canadian students sued the federal government after the loss of their personal information. These students received student loans through the Canada Student Loans Program and provided personal information as part of the approval process for receiving the loans. The personal information was being held temporarily on a hard drive and stored in an employee’s desk. The information went missing and was not recovered by the time the Federal Court of Appeal made its decision.

- The Federal Court found that the class action could be certified even though the students could not prove specific tangible damages but could only prove intangible damages. This decision was upheld on appeal. Organizations should therefore be aware that data breaches can expose organizations to potentially large damage awards under Canadian law, even if the action is based on allegations of recklessness and tangible damages have not been proved; even an award of C$10,000 to each of the 583,000 members of the class would result in a damages award of over C$5 billion.
In January 2015, the Canadian federal government tabled Bill C-51, known by its short title the Anti-Terrorism Act, 2015. The bill would enact the Security of Canada Information Sharing Act, which is designed to remove the information sharing barriers among federal public bodies on the basis of protecting national security interests. In particular, the legislation would generally allow a federal institution to, on its own initiative or upon request, disclose information to the prescribed federal institution if the information is relevant to the recipient’s jurisdiction in respect of “activities that undermine the security of Canada”. Such activities are defined broadly to include those relating to a wide range of purposes, such as espionage, terrorism, proliferation of weapons and interference with critical infrastructure.

The bill would also amend the Canadian Security Intelligence Service Act such that, if there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Canadian Security Intelligence Service (“CSIS”) may take reasonable and proportional measures inside or outside of Canada to reduce the threat. CSIS would be required to obtain a warrant where those measures will contravene a right or freedom guaranteed by the Canadian Charter of Rights and Freedoms. The bill would also authorize the Federal Court of Canada to issue assistance orders requiring third parties to assist with the measures taken by CSIS.

The bill would make a number of other security-related amendments, including the creation of an offence for knowingly advocating or promoting the commission of terrorism offences in general, and the establishment of a more formal and expanded “do not fly list” targeted at persons who may engage in an act that poses a threat to transportation security or who may travel by air for the purpose of committing a terrorism offence.

2. Emerging Privacy Issues and Trends

In January 2015, the OPC held a meeting with industry stakeholders to discuss certain privacy issues that it views as being important areas of focus in the next five years. The areas identified by the OPC are as follows:

- **Economics of Personal Information**

  This relates to the exchange of personal information for services such as applications and access to free offerings, and related issues of transparency, fair information practices and lack of regulation.
• **Government Services and Surveillance**
  This relates to the privacy risks and benefits of the Government of Canada’s consideration of adopting new technologies and increasing information sharing between departments, government and jurisdictions.

• **Protecting Canadians in a Borderless World**
  This relates to privacy issues around cross-border transfers of data and the Office of the Privacy Commissioner’s increasing coordination with international privacy regulators in conducting investigations.

• **Reputation and Privacy**
  This relates to questions around profiling individuals and how to suppress and refute negative, outdated or inaccurate information about oneself that has been shared publicly.

• **The Body as Information**
  This relates to the security and privacy issues accompanying the prevalence of sensors, wearables, and other technologies used to extract information from the body.

• **Strengthening Accountability and Privacy Safeguards**
  This reflects an increased focus on ensuring that the government and private organizations remain accountable for their privacy practices and secure the personal information under their control/custody.

3. **Law Applicable**

   *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, SC 2010, c 23 ("CASL").*

   *Personal Information Protection and Electronic Documents Act, SC 2000, c 5 ("PIPEDA").*


   *Order Binding Certain Agents of Her Majesty for the Purposes of Part 1 of the Personal Information Protection and Electronic Documents Act, SOR/2001-8.*


   *Organizations in the Province of British Columbia Exemption Order, SOR/2004-220.*
Organizations in the Province of Quebec Exemption Order, SOR/2003-374.


Regulations Specifying Investigative Bodies, SOR/2001-6.


Principles set out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSAQ830-96 (“Sch. 1”).

PIPEDA applies to all collection, use, or disclosure of Personal Information (as defined in Section 4(a) below) in the course of commercial activity by:

- federally-regulated private sector organizations, including those in the telecommunications, broadcasting, and inter-provincial transportation and banking sectors, with respect to both customer and employee Personal Information; and
- organizations that trade in Personal Information across provincial or national borders for consideration.

An “organization” is defined to include an association, a partnership, a person, and a trade union. However, in provinces where a law has been passed that is substantially similar to PIPEDA, organizations and their collection, use, or disclosure activities within the province that are covered by the provincial law are exempted from the application of PIPEDA. Provincial private sector privacy legislation has been deemed substantially similar to PIPEDA in British Columbia, Alberta, Quebec, and, in relation to personal health information, Ontario, New Brunswick and Newfoundland and Labrador (Nova Scotia is expected to be added to this list in regards to personal health information). PIPEDA continues to apply to employee Personal Information of federally-regulated businesses everywhere in Canada, and to inter-provincial and international collection, use, or disclosure of Personal Information.

4. Scope of the Law

a. Personal Data

PIPEDA applies to personally identifiable information (“Personal Information”) about an identifiable individual (“Data Subject”), i.e., any factual or subjective information, recorded or not about a Data Subject. Financial, health, employment, consumer contact and preferences data typically fall within the definition of Personal Information. Personal Information includes personal health information, which is defined as information about a Data Subject’s mental or physical health, including information concerning health services provided and information about tests and examinations. Personal Information generally does not include the name, title or business address or telephone number of an employee of an organization.
PIPEDA applies broadly to the collection, use, disclosure, handling and care, and any other processing of Personal Information in any form or representation, including electronic data recorded or stored on any medium, computer system, or other similar device, and that can be read or perceived by a person, system, or other device (e.g., display, printout, audio/video recording, or other data output).

b. Data Processing

“Processing” is not expressly defined in PIPEDA but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of the Data Controller, including handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating, and deleting Personal Information – whether on a manual or automated basis.

c. Processing by Data Controllers

PIPEDA applies to Personal Information that:

- the organization collects, uses or discloses in the course of commercial activities; or
- is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

d. Jurisdiction/Territoriality

PIPEDA applies to all Personal Information collected or processed in Canada, subject to the qualifications noted in Section 3 above regarding provinces where a law has been passed that has been deemed substantially similar to PIPEDA.

Federal and provincial public sector privacy statutes apply to personal information in records held by government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.

e. Sensitive Personal Data

In determining the requisite form of consent to be obtained, organizations are required to take into account the sensitivity of the Personal Information. Accordingly, the form of the consent sought by the organization below may vary, depending upon the circumstances and the type of Personal Information to be collected, used or disclosed. Although any Personal Information can be sensitive, depending on the context, note that some types of Personal Information, such as medical records and income records, are almost always considered to be sensitive. Employment and health care are generally matters
of provincial regulation, and as such are not covered by PIPEDA for provincially regulated companies.

f. Employee Personal Data
Employee Personal Information is treated in the same manner as other Personal Information. Employee Personal Information typically does not include an employee’s name, title, or business address or telephone number. Note, however, that PIPEDA does not apply to employee Personal Information of a provincially regulated organization, because regulation of the processing of such Personal Information falls under the jurisdiction of applicable provincial privacy laws.

5. Consent
a. General
The consent of a Data Subject is required for the collection, use, or disclosure of Personal Information.

Consent must be obtained before or at the time of collection. When Personal Information that has been collected is to be used for a purpose not previously identified, consent of the Data Subject shall be obtained prior to use by informing the Data Subject of such new purpose.

PIPEDA does not necessarily require that the consent be obtained in writing. In determining the appropriate form of consent to be obtained from a Data Subject, consideration should be given to the reasonable expectations of the Data Subject, circumstances surrounding the collection, and sensitivity of the Personal Information involved.

However, when consent is implied or obtained orally, for evidentiary reasons, an organization should as a matter of course keep some record of the consent obtained. The Privacy Commissioner of Canada recommends that express consent be used whenever possible and in all cases when the Personal Information is considered to be sensitive.

Relying on express consent protects both the Data Subject and the organization.

At a minimum, a request for consent should specify in plain language: the nature of the Personal Information to be collected, used, or disclosed; the specific uses to which the Personal Information will be put by receiving parties; the identity of the parties, if any, to whom Personal Information is to be disclosed; the channels available for the Data Subject to amend or withdraw his or her consent (e.g., e-mail, regular mail, 1-800 number, etc.).

A Data Subject should only be required to consent to the collection, use, or disclosure of Personal Information in order to fulfil the explicitly specified and legitimate purposes.
Data Subjects can give consent in many ways. Data Subjects can withdraw consent at any time. Consent can be given by an authorized representative (such as a legal guardian or a Data Subject having a power of attorney).

Consent clauses should be easy to find, use clear and straightforward language, avoid using blanket categories for purposes, uses, and disclosures, and be as specific as possible about which organizations handle the Personal Information. Consent shall not be obtained through deception.

In certain circumstances, Personal Information may be collected, used, or disclosed without the knowledge and consent of the Data Subject. For example, consent need not be obtained where legal, medical, or security reasons make it impossible or impractical to seek consent. Similarly, when the Personal Information is being collected for the detection and prevention of fraud or for law enforcement, it may not be necessary to obtain consent of the Data Subject, as doing so might defeat the purpose of collecting the Personal Information.

b. Sensitive Data
An organization should seek express consent from a Data Subject when the Personal Information involved is likely to be considered sensitive, having regard to the reasonable expectations of the Data Subject. This is intended to ensure that the consent is given freely and is provided on an informed basis.

c. Minors
For a Data Subject who is a minor, consent may be obtained from a legal guardian or person having power of attorney.

d. Employee Consent
Federal works, undertakings and business (e.g., airlines and banks) may collect, use, and disclose the personal information of an employee without his or her consent where it is necessary to establish, manage, or terminate the employment relationship as long as the employee is informed of such collection, use, or disclosure. All the requirements set out by PIPEDA for the giving of consent by any Data Subject shall equally apply to consent given by employees covered by PIPEDA.

e. Online/Electronic Consent
Electronic consent will usually suffice if appropriate steps are taken to ensure that a Data Subject is aware of the Data Controller’s data processing practices and policies (e.g., an appropriately accessible hyperlink – directly above a consent button).
6. Notice Requirements

Under PIPEDA, an organization is required to ensure that individuals are able to acquire information about an organization’s policies and practices without unreasonable effort. The organization shall also ensure that this information is in a form that is generally understandable, and includes:

- the name or title, and the address, of the person who is accountable for the organization’s policies and practices and to whom complaints or inquiries can be forwarded;
- the means of gaining access to Personal Information held by the organization;
- a description of the type of Personal Information held by the organization, including a general account of its use;
- a copy of any brochures or other information that explains the organization’s policies, standards, or codes; and
- what Personal Information is made available to related organizations (e.g., subsidiaries).

7. Processing Rules

An organization that processes Personal Data must: limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Information once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject; be informed by an organization of how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

No formal registration requirements apply.

10. Data Protection Officers

Under PIPEDA, an organization is responsible for Personal Information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the principles. Upon request, the organization shall disclose the identity of the designated individual(s).
Notwithstanding the fact that the designated individual(s) are accountable for the organization's compliance with the principles, other individuals within the organization may be responsible for the day-to-day collection and processing of Personal Information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

11. International Data Transfers

Under PIPEDA, there are no formal restrictions on transfers of Personal Information from Canada to other jurisdictions. However, an organization is obligated to put appropriate data transfer agreements or other measures in place to address the obligations of third-party Data Processors and recipients of Personal Information in the context of onward transfers.

12. Security Requirements

Organizations are required: to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Under PIPEDA, an organization shall be responsible for Personal Information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by the third party.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings, publication of breaches, and/or private rights of action.

15. Data Security Breach

On an unspecified date in the future, amendments establishing a data breach notification requirement under PIPEDA will come into force. According to this new requirement, where there is a security breach and it is reasonable in the circumstances to believe that the breach could create a risk of significant harm, an organization must notify the OPC, any affected individual(s), and any third-party organizations that may be able to reduce the possible harm. The disclosure to the OPC and other third parties may be made without the prior consent of the individual where it is made for the purpose of reducing harm to the individual(s) affected by the security breach. The notification must contain
sufficient information to allow the affected individual(s) to understand the significance and consequence of the breach to allow them to take any necessary steps to prevent or mitigate such harm. Any notice must be conspicuous and given directly to the individual in the prescribed form and manner as soon as is feasible.

PIPEDA defines significant harm as “bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property”.

Organizations must also keep and maintain records of all security breaches and provide these records to the OPC upon request by the OPC.

An organization that is involved in a data breach situation may be subject to: a suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions and/or class actions, and/or a criminal prosecution.

16. Accountability

There is currently no requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-blower hotline

Whistle-blower hotlines may be established in Canada provided that they are in compliance with local laws.

18. E-discovery

To the extent that Personal Information is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with PIPEDA. An organization should take privacy-related issues into consideration prior to the commencement and during the course of litigation.

Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization shall use contractual or other means to ensure that Personal Information and such system are protected while being processed by the third party.

19. Anti-Spam Filtering

Section 184(1) of the Criminal Code sets out the general rule that it is illegal to wilfully intercept a private communication, 'Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a
private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.’

Therefore, organizations should ensure that the introduction and the implementation of a spam-filtering solution is in compliance with PIPEDA and the Criminal Code.

20. Cookies

There are specific laws/rules in Canada that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent is not considered valid consent.
Alberta, Canada

1. Recent Privacy Developments

The Government of Alberta Implements an Amended Provincial Personal Information Protection Act

On December 17, 2014, amendments to the Alberta Provincial Personal Information Protection Act ("Alberta PIPA") came into force. The amendments, which respond to a decision of the Supreme Court of Canada that struck down the statute in its entirety, allow labour unions in the context of a labour dispute to engage in reasonable collection, use or disclosure of personal information without an individual’s consent, provided the following conditions are met:

- the collection, use, or disclosure of the personal information is for the purpose of informing or persuading the public about a matter of significant public interest or importance relating to a labour relations dispute;
- the collection, use, or disclosure of the personal information is reasonably necessary for that purpose; and
- the collection, use, or disclosure of the personal information without consent is reasonable in the context, taking into consideration all relevant considerations, including the nature and sensitivity of the personal information.

The Supreme Court of Canada had ruled in Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401, 2013 SCC 62, that the version of the Alberta PIPA then in effect was unconstitutional. The case arose in the context of a strike lasting 305 days. During the course of the dispute, both the union and the employer videotaped and photographed individuals crossing the picket line. The union used signs to notify individuals in the picketing area that they were being recorded, and images of persons crossing the picket line were used in union newsletters, posters and pamphlets. An adjudicator appointed by the Alberta Information and Privacy Commissioner concluded that the union’s collection, use and disclosure of the information was not authorized by the Alberta PIPA.

The issue before the Supreme Court of Canada was whether the Alberta PIPA unjustifiably limits a union’s right to freedom of expression in the context of a strike. In deciding that it does, the Supreme Court of Canada criticized the legislation for limiting the collection, use and disclosure of personal information (other than with consent) without regard for the nature of the personal information, the purpose for which it is collected, used or disclosed, and the situational context for that information. Finding that the Alberta PIPA failed to achieve a constitutionally acceptable balance between the privacy
interests of individuals and unions’ freedom of expression, the Supreme Court of Canada struck down the Alberta PIPA and gave the Government of Alberta 12 months to amend the legislation accordingly.

**Alberta, Federal and British Columbia Privacy Commissioners Issue Guidelines for Obtaining Meaningful Consent in the Online Environment**

In May 2014, the Office of the Information and Privacy Commissioner of Alberta (“OIPCA”), in collaboration with its federal and British Columbian counterparts, jointly issued the “Guidelines for Online Consent” (“the Guidelines”) to help organizations understand their legal obligations around obtaining meaningful consent in the online environment. For more information, see the “Recent Privacy Developments” in the Canada chapter.

**Alberta Privacy Commissioner Signs Open Letter Calling for Mandatory Privacy Policies in Mobile Apps after Participating in Global Privacy Enforcement Network Privacy Sweep**

In May 2014, the OIPCA engaged in the second annual Global Privacy Enforcement Network Privacy Sweep in concert with 25 other privacy authorities around the world. This year’s Privacy Sweep focused on how transparent organizations are regarding the privacy practices of their mobile applications. The OIPCA evaluated 21 Alberta-based mobile apps in the private, public and health sectors (of 1,211 apps examined globally). Following the sweep, the OIPCA signed a joint open letter with 22 other privacy authorities from around the world addressed to mobile application marketplaces calling for, among other things, mandatory privacy policies in mobile applications that collect personal information. For more information on the privacy sweep, see the “Recent Privacy Developments” in the Canada chapter.

2. Emerging Privacy Issues and Trends

In its strategic business plan for 2015-2018, the OIPCA has stressed that it will take a more proactive approach to privacy law enforcement and has highlighted the following, among others, as items that it may focus on:

- Compliance with data breach
- Compliance with privacy impact assessments under Alberta’s personal health information laws
- The privacy implications of the use and prevalence of:
  - Biometrics
  - Mobile devices
  - Geo-location tracking software
  - Interoperability of information systems
3. Law Applicable

**Personal Information Protection Act**, SA 2003, c P-6.5 ("Alberta PIPA") and related regulations.

**Health Information Act**, RSA 2000, c H-5 and related regulations.

This chapter focuses on the Alberta PIPA and related regulations.

The purpose of the Alberta PIPA is to govern the means by which private sector organizations handle personal information, and ensure this occurs in a manner that recognizes both the right of an individual ("Data Subject") to have his or her personally identifiable information ("Personal Information") protected and the need of organizations to collect, use or disclose Personal Information for purposes that are reasonable.

An organization includes a corporation, an association that is not incorporated, a trade union, a partnership and an individual acting in a commercial way (e.g., an individual running an unincorporated business).

4. Scope of the Law

a. **Personal Data**

The Alberta PIPA applies to information about an identifiable individual ("Personal Information") (e.g., name, home address, home phone number, ID numbers, physical description, educational qualifications, blood type, etc.).

“Business contact information” is a subset of Personal Information. It includes a Data Subject’s name, position or title, business telephone number, business email address, and other business contact information. The Alberta PIPA does not apply to business contact information when it is collected, used or disclosed for the purpose of contacting an individual in his or her business capacity.

The Alberta PIPA applies to a “record,” which means a record of information in any form or in any medium, whether in written, printed, photographic, electronic, or any other form, but does not include a computer program or other mechanism that can produce a record.
b. Data Processing

Processing is not expressly defined in the Alberta PIPA but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of the Data Controller, including the handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating, or deleting of Personal Information - whether on a manual or automated basis.

c. Processing by Data Controllers

The Alberta PIPA applies to every organization and with respect to all Personal Information.

The Alberta PIPA does not apply:

- if the collection, use, or disclosure of Personal Information is for personal or domestic purposes;
- if the collection, use, or disclosure of Personal Information is for artistic, literary, or journalistic purposes;
- if the collection, use, or disclosure of business contact information is for the purpose of contacting an individual in that individual’s capacity as an employee of an organization;
- if the Personal Information is in the custody or control of a “public body”;
- if the Freedom of Information and Protection of Privacy Act applies;
- if the information is health information as defined in the Health Information Act;
- if the information is about an individual who has been dead for 20 years or more or in a record that is 100 years old or older; or
- if the information is Personal Information in court files.

An organization is responsible for all of the Personal Information that is either in its custody or under its control. Where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person’s compliance with the Alberta PIPA. The organization must designate one or more individuals to be responsible for ensuring the organization complies with the Alberta PIPA.

An organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under the Alberta PIPA, and make information about such policies and practices available on request.
d. Jurisdiction/Territoriality

The Alberta PIPA applies to provincially regulated businesses, non-profit organizations (only when they collect, use or disclose Personal Information in connection with a “commercial activity”), trade unions and other organizations in Alberta. “Commercial activity” means a transaction, act or conduct that has a commercial character to it, such as selling, bartering or leasing donor, membership or other fundraising lists. It also includes operating a private school or college or an early childhood services program.

However, PIPEDA will in most instances still apply to provincially regulated organizations when they transfer Personal Information across Alberta’s borders, in the course of commercial activity (i.e., for consideration). Organizations should thus consider obtaining consent, as appropriate, in connection with such trans-border transfers.

PIPEDA will also still apply to federally-regulated businesses in Alberta.

Federal and provincial public sector privacy statutes apply to personal information in records held by government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.

e. Sensitive Personal Data

The form of the consent sought by the organization pursuant to Section 5 below may vary, depending upon the circumstances and the type of information to be collected, used, or disclosed. In determining the form of consent to use, organizations shall take into account the sensitivity of the information.

Although some information (for example, health and financial information) is almost always considered to be sensitive, any information can be sensitive depending on the context. In such circumstances, as a best practice, organizations should obtain clear and express consent.

f. Employee Personal Data

An “Employee” includes an apprentice, a volunteer, a participant, a work experience or co-op student and an individual acting as an agent for an organization, employed by the organization or who performs a service for the organization as a partner or a director, officer or other office-holder of the organization, whether or not the individual is paid.

“Employee Personal Information” means, in respect to an individual who is a potential, current or former employee of an organization, Personal Information that is reasonably required by an organization to establish, manage or end an employment or volunteer work relationship, or to manage a post-employment relationship.
5. Consent

a. General

An organization generally must not collect, use or disclose Personal Information about a Data Subject without first obtaining consent.

A Data Subject may give consent subject to any reasonable terms, conditions or qualifications established, set, approved by or otherwise acceptable to the Data Subject.

Consent may not be obtained by providing false or misleading information regarding the collection, use or disclosure of information through deception.

The Alberta PIPA recognizes the following types of consent: express consent, implied consent; and opt-out consent.

The Alberta PIPA does not require an organization to provide notice when relying on implied consent to collect Personal Information.

An organization may not collect, use or disclose Personal Information for a different purpose than the purpose or purposes for which it was collected. A Data Subject can consent to an organization collecting his or her Personal Information from another organization.

A Data Subject is deemed to have consented to the collection of his or her Personal Information by an organization if the collection took place prior to 1 January 2004, and such consent may be relied upon where the Personal Information is used or disclosed for the purposes for which it was originally collected.

A Data Subject can change or withdraw consent by giving the organization reasonable notice, as long as doing so does not contravene a legal duty or obligation between the Data Subject and the organization. On receipt of such notice, an organization must inform the Data Subject of the likely consequences to the Data Subject of withdrawing consent. An organization must not prohibit a Data Subject from withdrawing consent to the collection, use or disclosure of Personal Information related to the Data Subject.

Following withdrawal of consent to the collection, use or disclosure of Personal Information by a Data Subject, the organization must stop collecting, using or disclosing the Personal Information unless the collection, use or disclosure is permitted without consent. A Data Subject may not withdraw consent given for the performance of a legal obligation.

The Alberta PIPA provides that neither an organization nor a Data Subject can impose a liability or an obligation on the other as a result of the withdrawal or variation of consent. An organization must not, as a condition of supplying a product or service, require a Data Subject to consent to the collection, use or
disclosure of Personal Information beyond what is necessary to provide the product or service.

An organization may collect, use or disclose Personal Information about a Data Subject without consent, if the collection, use and disclosure is clearly in the interests of the Data Subject:

- when another Act or regulation requires or allows for collecting information without consent;
- when the Personal Information is collected in accordance with the provisions of a treaty;
- when it relates to a subpoena, warrant, or court order;
- when it is provided by a public body;
- when it is necessary for medical treatment;
- when the collection is for an investigation or a proceeding;
- when the Personal Information is publicly available;
- when the organization is a credit reporting agency;
- when it is required or authorized by law;
- for disclosures without consent;
- for the collection of a debt; or
- for transfer of Personal Information to a third party.

Under certain circumstances, a trade union may also collect personal information about an individual without his or her consent for the purpose of informing or persuading the public about a significant matter relating to a labour relations dispute involving the trade union.

An organization may disclose Personal Information about its employees, customers, directors, officers, or shareholders without their consent to a prospective party in a business transaction. A business transaction is defined to mean the purchase, sale, lease, merger, amalgamation, acquisition, or disposal of an organization (or part of an organization) or any business or activity or business asset of an organization. If a business transaction does not proceed or is not completed, a prospective party must destroy or return to the organization any Personal Information that the prospective party collected about the employees, customers, directors, officers, and shareholders of the organization. An organization may not disclose Personal Information in a business transaction where the primary purpose, objective, or result of the transaction is the purchase, sale, lease, transfer, disposal, or disclosure of Personal Information.
b. Sensitive Data

An organization should seek express consent when Personal Information is likely to be considered sensitive, having regard to the reasonable expectations of the Data Subject. This is intended to ensure that the consent is given freely and is provided on an informed basis. Thus, at a minimum, a request for consent should refer to (i) the nature of the information to be collected, used or disclosed; (ii) the specific uses to which the information will be put by the parties receiving it; and (iii) the identity of the parties to whom information is to be disclosed, as applicable. A request for consent should also specify, in simple terms, the channels that are available (e.g., e-mail, regular mail, 1-800 number, etc.) for the Data Subject to amend or withdraw his or her consent.

The more sensitive the Personal Information is, the greater the likelihood that express consent will be required for its collection, use, and disclosure.

c. Minors

The guardian of a minor may give or refuse consent to the collection, use and disclosure of Personal Information of the minor if the minor is incapable of exercising that right (i.e., if the minor is incapable of understanding his or her rights under the Alberta PIPA and the consequences of exercising them).

d. Employee Consent

The Alberta PIPA permits an organization to collect, use or disclose Employee Personal Information without consent for reasonable purposes related to managing or recruiting personnel. “Managing personnel” means the carrying out of that part of human resource management relating to the duties and responsibilities of employees. It can also refer to administering personnel and includes activities such as payroll and succession planning.

Consent is required for the collection by the employer of Personal Information that does not constitute Employee Personal Information, such as information collected in relation to charitable donations, personal family issues or non-work related health, religious or financial issues.

An organization shall collect, use or disclose Employee Personal Information only if it is for a reasonable purpose, the information relates to the employment or volunteer work relationship and the organization has provided the Data Subject with reasonable notification before collection, use or disclosure of the information.

Where an organization outsources “back office” human resources functions such as payroll or administration, the Alberta PIPA may also permit the contracting organization to collect the Employee Personal Information without consent.
e. **Online/Electronic Consent**

Consent given or transmitted by electronic means will qualify as “written consent” only where the receiving organization produces or is capable of producing a version of that consent in paper form. Organizations that make use of paperless and/or signature-less contracts via their websites must ensure that they can produce evidence or paper versions of the consent upon request.

6. **Notice Requirements**

An organization that collects Personal Information generally must or should provide Data Subjects with information about the organization’s identity, the types of Personal Information collected, the purposes for collecting the Personal Information, the organization’s privacy practices (which must be clear and transparent), third parties to which the organization will disclose the Personal Information, the rights of the Data Subject, how the Personal Information is to be retained, where the Personal Information is to be transferred, where the Personal Information is to be stored, how to make an enquiry or file a complaint, how to access and/or correct the Data Subject’s Personal Information, the duration of the proposed processing, and the means of transmission of the Personal Information.

7. **Processing Rules**

An organization that processes Personal Information must limit the use of the Personal Information to those activities that are necessary to fulfil the identified purpose(s) for which the Personal Information was collected, and delete/destroy/anonymize Personal Information once the stated purposes have been fulfilled and legal obligations met.

8. **Rights of Individuals**

Data Subjects have the general right to be informed by an organization of the Personal Information that the organization holds about the Data Subject, and how the Data Subject’s Personal Information will be used and disclosed; access the Data Subject’s Personal Information, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Information; and request the deletion and/or destruction of the Data Subject’s Personal Information.

9. **Registration/Notification Requirements**

An organization that collects and processes Personal Data is not required to register, file and notify the appropriate data authority.

10. **Data Protection Officers**

An organization must designate one or more individuals to be responsible for ensuring that the organization complies with the Alberta PIPA.
11. International Data Transfers

Under the Alberta PIPA, there are no formal restrictions on transfers of Personal Information from Canada to other jurisdictions. However, organizations are required to notify individuals if they use service providers outside Canada to collect and/or process Personal Information. As the definition of “service providers” is quite broad and includes affiliated entities, it is recommended that appropriate data transfer agreements be put in place to address the obligations of recipients of Personal Information in the context of onward transfers.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Information in its possession and control is protected from unauthorized access and use, and implement appropriate physical, technical and organizational security safeguards to protect Personal Information.

13. Special Rules for Outsourcing of Data Processing to Third Parties

An organization is responsible for Personal Information that is in its custody or under its control and where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person’s compliance.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints; data authority investigations/audits; data authority inquiries and orders; administrative fines, penalties or sanctions; seizure of equipment or data; civil actions/private rights of action; class actions; and prosecution for offences.

15. Data Security Breach

Alberta is the first Canadian jurisdiction to require mandatory data security breach notification in the private sector. Organizations are required to report incidents of security breach to the Information and Privacy Commissioner of Alberta when there is a real risk of significant harm to an individual and the Commissioner can require such organizations to notify affected individuals.

An organization that is involved in a data breach situation may be subject to various penalties as noted above under ‘Enforcement and Sanctions’.

16. Accountability

There is currently no requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Information.
17. Whistle-blower hotline
Whistle-blower hotlines may be established in Alberta provided that they are in compliance with local laws.

18. E-discovery
To the extent that Personal Information is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with the Alberta PIPA. An organization should take privacy-related issues into consideration prior to the commencement and during the course of litigation.

Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization is required to use contractual or other means to ensure that Personal Information and the system employed are protected while being processed by the third party.

19. Anti-Spam Filtering
Subsection 184(1) of the Criminal Code (Canada) sets out the general rule that it is illegal to wilfully intercept a private communication: ‘Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.’

Therefore, the organization shall ensure that the introduction and implementation of a spam-filtering solution is in compliance with the Alberta PIPA and the federal Criminal Code.

20. Cookies
There are specific laws/rules in Alberta that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent is not considered valid consent.
1. Recent Privacy Developments

**British Columbia Supreme Court orders search results removed globally based on the “right to be forgotten” principle**

In June 2014, the British Columbia Supreme Court (“BCSC”) ordered an online search engine to remove a group of websites from both its Canadian domain, and its global search index. The case, *Equustek Solutions Inc. v. Jack*, 2014 BCSC 1063, affirmed by the British Columbia Court of Appeal, did not have a privacy issue at its core and mostly concerned the advertising of a counterfeit item in search results. However, the BCSC relied on a well-known decision of the European Court of Justice to support an order with global effect. In that decision, the European Court of Justice recognized that individuals have a right to be forgotten in the results of an online search. In order to give effect to this right, the BCSC stated that in certain instances it has the ability to order a search engine to remove all mention to infringing data from its service. While the European Court of Justice limited its order to Europe, the BCSC placed no such geographical limitation on its order.

The BCSC reasoned that if a search engine does business by advertising in Canada, the Court has jurisdiction over its global activities where a connection between the local activity and the global activity exists. As such, the decision contributes to the increasing attention on the nexus between local law and global access to information, including the potential extraterritorial jurisdiction of domestic statutes and courts.

**British Columbia, Federal and Alberta Privacy Commissioners Issue Guidelines for Obtaining Meaningful Consent in the Online Environment**

In May 2014, the Office of the Information and Privacy Commissioner (“OIPCBC”), in collaboration with its federal and Albertan counterparts, jointly issued the “Guidelines for Online Consent” (“the Guidelines”) to help organizations understand their legal obligations around obtaining meaningful consent in the online environment. For more information, see the “Recent Privacy Developments” in the Canada chapter.

**British Columbia Privacy Commissioner Signs Open Letter Calling for Mandatory Privacy Policies in Mobile Apps after Participating in Global Privacy Enforcement Network Privacy Sweep**

In May 2014, the OIPCBC engaged in the second annual Global Privacy Enforcement Network Privacy Sweep in concert with 25 other privacy authorities around the world. This year’s Privacy Sweep focused on how transparent organizations are regarding the privacy practices of their mobile
applications. The OIPCBC evaluated 15 financial apps popular in B.C. (of 1,211 apps examined globally), such as consumer expense trackers, budget and debt management apps, mortgage calculators, receipt scanners, and banking apps. The OIPCBC reported that 54% of the apps it examined failed to comply with notice and consent requirements under the British Columbia Personal Information Protection Act (“BC PIPA”). Following the sweep, the OIPCA signed a joint open letter with 22 other privacy authorities from around the world addressed to mobile application marketplaces calling for, among other things, mandatory privacy policies in mobile applications that collect personal information. For more information on the privacy sweep, see the “Recent Privacy Developments” in the Canada chapter.

2. Emerging Privacy Issues and Trends

In its most recent budget submission, the OIPCBC indicated that its priorities for 2015-2016 may include the privacy legal implications of:

- modern digital technologies that collect, use and disclose personal health information
- the use of video and audio surveillance systems
- auditing public bodies to identify and address privacy vulnerabilities

**Spam** – Federal anti-spam legislation came into force on July 1, 2014, and the provisions thereunder that regulate the installation of computer programs came into force on January 15, 2015. For more information, see the summary of Canada’s Anti-Spam Legislation (CASL) in the Canada chapter.

**Tips and Guidance for IT Security and Employee Privacy**

In June 2015, the OIPCBC released a regulatory guidance document that outlines the privacy issues that employers should consider before implementing information technology (“IT”) security tools that collect the personal information of employees. The document summarizes the application of privacy law in British Columbia in the employment context and sets out ten tips to help employers protect the personal information of their employees, including (1) completing a privacy impact assessment during the planning stages of implementing new IT tools; (2) ensuring IT and procurement staff consult the privacy officer when considering and implementing new IT tools; (3) providing notice of updated information practices to employees; (4) avoiding the continuous, real-time collection of personal information about employees; (5) having updated privacy training programs in place; and (6) evaluating the effectiveness of IT security programs on an ongoing basis.
3. Law Applicable

**Personal Information Protection Act**, SBC 2003, c 63 (“BC PIPA”) and related regulations.

The purpose of the BC PIPA is to govern the collection, use, and disclosure of Personal Information by organizations in a manner that recognizes both the right of individuals to protect their Personal Information and the need of organizations to collect, use, or disclose Personal Information for purposes that a reasonable person would consider appropriate in the circumstances.

An organization includes a person (which at law includes corporations), an unincorporated association, a trade union, a trust, or a not-for-profit organization. It excludes a “private trust” and an individual “acting as an employee.”

4. Scope of the Law

**a. Personal Data**

The BC PIPA applies to personally identifiable information (“Personal Information”) about an identifiable individual (“Data Subject”) and includes employee Personal Information, but does not include:

- business contact information; or
- work product information.

The BC PIPA applies to a “Document” which includes:

- a thing on or by which information is stored; and
- a document in electronic or similar form.

The BC PIPA applies broadly to the collection, use, disclosure, handling and care, and any other processing of Personal Information in any form or representation, including electronic data recorded or stored on any medium, computer system or other similar device, and that can be read or perceived by a person, system, or other device (e.g., display, printout, audio/video recording, or other data output). The BC PIPA does not apply to general information used to operate the organization’s business.

**b. Data Processing**

Processing is not expressly defined in the BC PIPA but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of the Data Controller, including the handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating, or deleting of Personal Information – whether on a manual or automated basis.
c. Processing by Data Controllers

The BC PIPA applies with limited exceptions to “every organization”. It covers commercial and not-for-profit activities and employee Personal Information within employment relationships. The BC PIPA does not apply:

- if collection, use or disclosure is for personal or domestic purposes, journalistic, artistic or literary purposes or where the federal PIPEDA or the Freedom of Information and Protection of Privacy Act (BC) applies;
- to Personal Information in a court document;
- to solicitor-client privilege information;
- to information available by law to a party or a proceeding; and
- to the collection of Personal Information that was collected prior to the date the legislation came into force.

The BC PIPA applies to Personal Information that:

- an organization considers appropriate in the circumstances; and
- is under its control, including Personal Information that is not in the custody of the organization.

PIPEDA applies to transfers of Personal Information across borders.

d. Jurisdiction/Territoriality

The BC PIPA applies to provincially regulated businesses, non-profit organizations, trade unions and other organizations in British Columbia. However, PIPEDA will in most instances still apply to provincially regulated organizations when they transfer Personal Information across British Columbia’s borders in the course of commercial activity (i.e., for consideration). Organizations should thus consider obtaining consent, as appropriate, in connection with such trans-border transfers. PIPEDA will also still apply to federally-regulated organizations operating in British Columbia.

Federal and provincial public sector privacy statutes apply to personal information in records held by government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.

e. Sensitive Personal Data

The form of the consent sought by the organization pursuant to Section 5 below may vary, depending upon the circumstances and the type of information to be collected, used or disclosed. In determining the form of consent to use, organizations are required to take into account the sensitivity of the information.
Although some information (for example, health and financial information) is almost always considered to be sensitive, any information can be sensitive depending on the context. In such circumstances, as a best practice, organizations should obtain clear and express consent.

f. Employee Personal Data
Employee Personal Information includes Personal Information about a Data Subject that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that Data Subject, but does not include Personal Information that is not about a Data Subject’s employment. Employee Personal Information does not include business contact information or work product information. The term “employees” is defined to include volunteers.

5. Consent
a. General
An organization must not collect, use or disclose Personal Information about a Data Subject without first obtaining consent. In order for a consent to be valid, the organization must inform the Data Subject, verbally or in writing, of the purpose for the collection of his/her Personal Information.

An organization must not, as a condition of supplying a product or service, require a Data Subject to consent to the collection, use or disclosure of Personal Information beyond what is necessary to provide the product or service.

Consent shall not be obtained by providing false or misleading information respecting the collection, use or disclosure of information through deception.

The BC PIPA recognizes the following types of consent: express consent, deemed consent, and opt-out consent.

An organization may not collect, use or disclose Personal Information for a purpose different than the purpose for which it was collected.

The BC PIPA does not apply to the collection, use, or disclosure of Personal Information that was collected before 1 January 2004. However, if the Personal Information that was collected before 1 January 2004, is used for a new purpose, fresh consent would have to be obtained in connection with such new purpose.

A Data Subject can cancel or change his or her consent by giving the organization reasonable notice. On receipt of such notice, an organization must inform the Data Subject of the likely consequences to the Data Subject of withdrawing his or her consent. An organization must not prohibit a Data Subject from withdrawing his or her consent to the collection, use, or disclosure of Personal Information. Pursuant to withdrawal of consent to the
collection, use, or disclosure of Personal Information by an organization, the organization must stop collecting, using, or disclosing the Personal Information unless continued collection, use, or disclosure is permitted without consent. A Data Subject may not withdraw consent given for the performance of a legal obligation or consent given to a credit reporting agency.

An organization may collect, use, or disclose Personal Information about a Data Subject without consent in certain situations (e.g., medical emergency, investigation, or required or authorized by law). An organization may disclose Personal Information about its employees, customers, directors, officers, or shareholders without their consent to a prospective party in a business transaction. A business transaction is defined to mean the purchase, sale, lease, merger, amalgamation, acquisition, or disposal of an organization (or part of an organization) or any business or activity or business asset of an organization. If a business transaction does not proceed or is not completed, a prospective party must destroy or return to the organization any Personal Information that the prospective party collected about the employees, customers, directors, officers, and shareholders of the organization. The organization is not authorized to disclose Personal Information to a party or prospective party for purposes of a business transaction that does not involve substantial assets of the organization other than this Personal Information. An organization may disclose, without the consent of a Data Subject, Personal Information for a research purpose, including statistical research and for archival or historical purposes.

b. Sensitive Data
An organization should seek express consent when Personal Information is likely to be considered sensitive, having regard to the reasonable expectations of the Data Subject. This is intended to ensure that the consent is given freely and is provided on an informed basis. Thus, at a minimum, a request for consent should refer to (i) the nature of the information to be collected, used, or disclosed; (ii) the specific uses to which the information will be put by the parties receiving it; and (iii) the identity of the parties to whom information is to be disclosed, as applicable. A request for consent should also specify, in simple terms, the channels that are available (e.g., e-mail, regular mail, 1-800 number, etc.) for the Data Subject to amend or withdraw his or her consent. It should be noted that the more sensitive the Personal Information is, the greater the likelihood that express consent will be required for its collection, use, and disclosure.

c. Minors
The guardian of a minor may give or refuse consent to the collection, use, and disclosure of Personal Information of the minor if the minor is incapable of exercising that right in the circumstances.
d. Employee Consent
An organization may collect, use, and disclose employee Personal Information without the consent of the Data Subject if the collection is reasonable for the purposes of establishing, managing, or terminating an employment relationship between the organization and the Data Subject. An organization must notify the Data Subject that it will be collecting employee Personal Information about the Data Subject and the purposes for the collection before the organization collects the employee Personal Information without the consent of the Data Subject.

e. Online/Electronic Consent
Electronic consent will suffice if appropriate steps are taken to ensure that a Data Subject is aware of the Data Controller’s data processing practices and policies (e.g., inclusion of an appropriately accessible hyperlink – directly above a consent button).

6. Notice Requirements
A organization that collects Personal Information generally must or should provide Data Subjects with information about: the organization’s identity, the types of Personal Information being collected, the purposes for collecting the Personal Information, its privacy practices (which must be clear and transparent), third parties to which the organization will disclose the Personal Information, the rights of the Data Subject, how the Personal Information is to be retained, where the Personal Information is to be transferred, where the Personal Information is to be stored, how to make an enquiry or file a complaint, how to access and/or correct the Data Subject’s Personal Information, the duration of the proposed processing and the means of transmission of the Personal Information.

7. Processing Rules
An organization that processes Personal Information must limit the use of the Personal Information to those activities that are necessary to fulfil the identified purpose(s) for which the Personal Information was collected, and delete/destroy/anonymize Personal Information once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Information that the organization holds about the Data Subject, and how the Data Subject’s Personal Information will be used and disclosed; access the Data Subject’s Personal Information, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Information; and request the deletion and/or destruction of the Data Subject’s Personal Information.
9. Registration/Notification Requirements
An organization that collects and processes Personal Data is not required to register, file and notify the appropriate data authority.

10. Data Protection Officers
An organization must designate one or more individuals to be responsible for ensuring compliance. The identity and contact information of the privacy officer(s) must be made available to the public. The privacy officer(s) may also be the contact person for answering questions about the BC PIPA and for handling access requests and complaints.

11. International Data Transfers
Under the BC PIPA, there are no formal restrictions on transfers of Personal Information from Canada to other jurisdictions. However, it is recommended that appropriate data transfer agreements be put in place to address the obligations of recipients of Personal Information in the context of onward transfers.

12. Security Requirements
Organizations are required: to take steps to ensure that Personal Information in its possession and control are protected from unauthorized access and use, and implement appropriate physical, technical and organizational security safeguards to protect Personal Information.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Under BC PIPA, an organization is responsible for personal information under its control, including Personal Information that is not in the custody of the organization.

Organizations that disclose Personal Information to third parties are required to use contractual or other means to protect Personal Information and comply with sector specific requirements. Organizations shall be liable together with the third party providers in case of breach by the latter.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints; data authority investigations/audits; data authority Inquiries and orders; administrative fines, penalties or sanctions; seizure of equipment or data; civil actions/private rights of action; class actions; and prosecution for offences.
15. Data Security Breach

While the BC PIPA does not create an explicit legal requirement to notify the B.C. Commissioner or affected individuals in the event of a data security breach, it obliges organizations to take reasonable security measure to protect Personal Information in their custody. The Information & Privacy Commissioner for British Columbia has also published guidance documents regarding privacy breaches and breach notification and privacy breaches which provide information on how to address data security breaches and what information to include if an organization decides to report the breach to the Commissioner or to affected individuals.

An organization that is involved in a data breach situation may be subject to various penalties as noted above under ‘Enforcement and Sanctions.”

16. Accountability

There is currently no requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Information.

17. Whistle-blower hotline

Whistle-blower hotlines may be established in British Columbia provided that they are in compliance with local laws.

18. E-discovery

To the extent that Personal Information is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with the BC PIPA. An organization should take privacy-related issues into consideration prior to the commencement and during the course of litigation.

Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization is required to use contractual or other means to ensure that Personal Information and the system employed are protected while being processed by the third party.

19. Anti-Spam Filtering

Subsection 184(1) of the Criminal Code (Canada) sets out the general rule that it is illegal to wilfully intercept a private communication, ‘Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.’
Therefore, the organization shall ensure that the introduction and implementation of a spam-filtering solution is in compliance with the BC PIPA and the federal Criminal Code.

20. Cookies

There are specific laws/rules in British Columbia that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a data subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent is not considered valid consent.
Manitoba, Canada

1. Recent Privacy Developments

*Manitoba Enacts Private Sector Privacy Law*

In 2013, the Manitoba government enacted The Personal Information Protection and Identity Theft Prevention Act ("Manitoba PIPITPA"), making it the fourth province along with British Columbia, Alberta and Québec to enact broadly applicable private sector privacy legislation. The Manitoba PIPITPA, which is not yet in force, will apply to all private sector organizations including corporations, unincorporated associations, unions, partnerships and individuals acting in a commercial capacity. The Manitoba PIPITPA generally requires organizations to obtain the consent of an individual before collecting, using or disclosing his or her Personal Information. The Manitoba PIPITPA also requires organizations to provide Data Subjects with reasonable access and correction rights and to take reasonable security precautions against privacy risks.

The Manitoba PIPITPA resembles the private sector privacy laws of Alberta and British Columbia in many ways, such as by establishing offences punishable by fines of up to CAD $100,000 and by providing exceptions for employers collecting, using and disclosing the Personal Information of employees under certain circumstances. An important distinction between the Manitoba PIPITPA and the privacy laws of Alberta and British Columbia is that it provides fewer circumstances in which an individual gives implied consent. For example, the privacy legislation of Alberta and British Columbia provide that consent is implied where the individual has an interest in a pension plan and the processing of Personal Information relates to enrollment or coverage under the plan. The Manitoba PIPITPA does not contain a similar provision.

The Manitoba PIPITPA will be administered in part by the Manitoba Ombudsman, who is currently responsible for investigating complaints and reviewing compliance with respect to The Freedom of Information and Protection of Privacy Act, which is Manitoba’s public sector privacy legislation, and The Personal Health Information Act, which relates to Manitoba’s health sector. Unlike the privacy commissioners of Alberta, British Columbia and Quebec, the Manitoba Ombudsman does not have the power to make orders respecting issues of legal compliance. The privacy regime in Manitoba is further complemented by the provincial *Privacy Act*, which creates a private cause of action for breach of privacy.
2. Emerging Privacy Issues and Trends

Spam – Federal anti-spam legislation came into force on July 1, 2014, and the provisions thereunder that regulate the installation of computer programs came into force on January 15, 2015. For more information, see the summary of Canada’s Anti-Spam Legislation (“CASL”) in the Canada chapter.

3. Law Applicable

The Personal Information Protection and Identity Theft Protection Act, CCSM c P33.7 (“Manitoba PIPITPA”) (not yet in force).

The Privacy Act, CCSM c P125.

Personal Health Information Act, CCSM c P33.5 and related regulations.

This chapter focuses on the Manitoba PIPITPA.

The purpose of the Manitoba PIPITPA is to govern the collection, use, and disclosure of Personal Information by organizations in a manner that recognizes both the right of individuals to protect their Personal Information and the need of organizations to collect, use, or disclose Personal Information for purposes that a reasonable person would consider appropriate in the circumstances.

An organization includes a person (which at law includes corporations), an unincorporated association, a trade union, a trust, or a not-for-profit organization. It excludes a “private trust” and an individual “acting as an employee.”

4. Scope of the Law

Please note that the Manitoba PIPITPA is not yet in force.

a. Personal Data

The Manitoba PIPITPA applies to Personal Information that can identify an individual (e.g., name, home address, home phone number, ID numbers) and information about a Data Subject (e.g., physical description, educational qualifications, blood type).

“Business contact information” is a subset of Personal Information. It includes a Data Subject’s name, position or title, business telephone number, business email address, and other business contact information. The Manitoba PIPITPA does not apply to business contact information when it is collected, used or disclosed for the purpose of contacting an individual in his or her business capacity.

The Manitoba PIPITPA applies to a “record,” which means a record of information in any form or in any medium, whether in written, printed, photographic, electronic, or any other form, but does not include a computer program or other mechanism that can produce a record.
b. **Data Processing**

Processing is not expressly defined in the Manitoba PIPITPA but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of the Data Controller, including the handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating, or deleting of Personal Information - whether on a manual or automated basis.

c. **Processing by Data Controllers**

The Manitoba PIPITPA applies to every organization and with respect to all Personal Information.

The Manitoba PIPITPA does not apply:

- if the collection, use, or disclosure of Personal Information is for personal or domestic purposes;
- if the collection, use, or disclosure of Personal Information is for artistic, literary, or journalistic purposes;
- if the collection, use, or disclosure of business contact information is for the purpose of contacting an individual in that individual’s capacity as an employee of an organization;
- if the Personal Information is in the custody or control of a “public body”;
- if the Freedom of Information and Protection of Privacy Act applies;
- if the information is health information as defined in the Personal Health Information Act;
- if the information is about an individual who has been dead for 20 years or more or in a record that is 100 years old or older; or
- if the information is Personal Information in court files.

An organization is responsible for all of the Personal Information that is either in its custody or under its control. Where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person’s compliance with the Manitoba PIPITPA. The organization must designate one or more individuals to be responsible for ensuring the organization complies with the Manitoba PIPITPA.

An organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under the Manitoba PIPITPA, and make information about such policies and practices available on request.
d. **Jurisdiction/Territoriality**

The Manitoba PIPITPA applies to provincially regulated businesses, non-profit organizations (only when they collect, use or disclose Personal Information in connection with a “commercial activity”), trade unions and other organizations in Manitoba. “Commercial activity” means a transaction, act or conduct that has a commercial character to it, such as selling, bartering or leasing donor, membership or other fundraising lists. It also includes operating a private school or college or an early childhood services program.

However, PIPEDA will in most instances still apply to provincially regulated organizations when they transfer Personal Information across Manitoba’s borders, in the course of commercial activity (i.e., for consideration). Organizations should thus consider obtaining consent, as appropriate, in connection with such trans-border transfers.

PIPEDA will also still apply to federally-regulated businesses in Manitoba.

Federal and provincial public sector privacy statutes apply to Personal Information in records held by government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.

e. **Sensitive Personal Data**

The form of the consent sought by the organization pursuant to Section 5 below may vary, depending upon the circumstances and the type of information to be collected, used, or disclosed. In determining the form of consent to use, organizations shall take into account the sensitivity of the information.

Although some information (for example, health and financial information) is almost always considered to be sensitive, any information can be sensitive depending on the context. In such circumstances, as a best practice, organizations should obtain clear and express consent.

f. **Employee Personal Data**

An “Employee” includes an apprentice, a volunteer, a participant, a work experience or co-op student and an individual acting as an agent for an organization, employed by the organization or who performs a service for the organization as a partner or a director, officer or other office-holder of the organization, whether or not the individual is paid.

“Employee Personal Information” means, in respect to an individual who is a potential, current or former employee of an organization, Personal Information that is reasonably required by an organization to establish, manage or end an employment or volunteer work relationship, or to manage a post-employment relationship.
5. Consent

a. General

An organization must not collect, use or disclose Personal Information about a Data Subject without first obtaining consent.

A Data Subject may give consent subject to any reasonable terms, conditions or qualifications established, set, approved by or otherwise acceptable to the Data Subject.

Consent shall not be obtained by providing false or misleading information regarding the collection, use or disclosure of information through deception.

The Manitoba PIPITPA recognizes the following types of consent: express consent; deemed consent; and opt-out consent.

The Manitoba PIPITPA does not require an organization to provide notice when relying on implied consent to collect Personal Information.

An organization may not collect, use or disclose Personal Information for a different purpose than the purpose for which it was collected. A Data Subject can consent to an organization collecting his or her Personal Information from another organization.

A Data Subject is deemed to have consented to the collection of his or her Personal Information by an organization if the collection took place prior to the date upon which the Manitoba PIPITPA comes into force, and such consent may be relied upon where the Personal Information is used or disclosed for the purposes for which it was originally collected.

A Data Subject can change or take back his or her consent by giving the organization reasonable notice, as long as doing so does not break a legal duty or promise between the Data Subject and the organization. On receipt of such notice, an organization must inform the Data Subject of the likely consequences to the Data Subject of withdrawing his or her consent. An organization must not prohibit a Data Subject from withdrawing his or her consent to the collection, use or disclosure of Personal Information related to the Data Subject.

Pursuant to withdrawal of consent to the collection, use or disclosure of Personal Information by a Data Subject, the organization must stop collecting, using or disclosing the Personal Information unless the collection, use or disclosure is permitted without consent. A Data Subject may not withdraw consent given for the performance of a legal obligation.

The Manitoba PIPITPA provides that neither an organization nor a Data Subject can impose a liability or an obligation on the other as a result of the withdrawal or variation of consent. An organization must not, as a condition of supplying a product or service, require a Data Subject to consent to the
collection, use or disclosure of Personal Information beyond what is necessary to provide the product or service.

An organization may collect, use or disclose Personal Information about a Data Subject without consent, if the collection, use and disclosure is clearly in the interests of the Data Subject:

- when another Act or regulation requires or allows for collecting information without consent;
- when the Personal Information is collected in accordance with the provisions of a treaty;
- when it relates to a subpoena, warrant, or court order;
- when it is provided by a public body;
- when it is necessary for medical treatment;
- when the collection is for an investigation or a proceeding;
- when the Personal Information is publicly available;
- when the organization is a credit reporting agency;
- when it is required or authorized by law;
- for disclosures without consent;
- for the collection of a debt; or
- for transfer of Personal Information to a third party.

b. **Sensitive Data**

An organization should seek express consent when Personal Information is likely to be considered sensitive, having regard to the reasonable expectations of the Data Subject. This is intended to ensure that the consent is given freely
and is provided on an informed basis. Thus, at a minimum, a request for consent should refer to (i) the nature of the information to be collected, used or disclosed; (ii) the specific uses to which the information will be put by the parties receiving it; and (iii) the identity of the parties to whom information is to be disclosed, as applicable. A request for consent should also specify, in simple terms, the channels that are available (e.g., e-mail, regular mail, 1-800 number, etc.) for the Data Subject to amend or withdraw his or her consent.

The more sensitive the Personal Information is, the greater the likelihood that express consent will be required for its collection, use, and disclosure.

c. **Minors**

The guardian of a minor may give or refuse consent to the collection, use and disclosure of Personal Information of the minor if the minor is incapable of exercising that right.

d. **Employee Consent**

The Manitoba PIPITPA permits an organization to collect, use or disclose Employee Personal Information without consent for reasonable purposes related to managing or recruiting personnel. “Managing personnel” means the carrying out of that part of human resource management relating to the duties and responsibilities of employees. It can also refer to administering personnel and includes activities such as payroll and succession planning.

Consent is still required for the collection by the employer of Personal Information that does not constitute Employee Personal Information, such as information collected in relation to charitable donations, personal family issues or non-work related health, religious or financial issues.

An organization shall collect, use or disclose Employee Personal Information only if it is for a reasonable purpose, the information relates to the employment or volunteer work relationship and the organization has provided the Data Subject with reasonable notification before collection, use or disclosure of the information.

Where an organization outsources “back office” human resources functions such as payroll or administration, the Manitoba PIPITPA may also permit the contracting organization to collect the Employee Personal Information without consent.

The Manitoba PIPITPA applies to Employee Personal Information in the same manner and to the same extent as it does to all other Personal Information.

e. **Online/Electronic Consent**

Consent given or transmitted by electronic means will qualify as “written consent” only where the receiving organization produces or is capable of producing a version of that consent in paper form. Organizations that make use of paper- and/or signature-less contracts via their websites must ensure
that they can produce evidence or paper versions of the consent upon request.

6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

7. Processing Rules
An organization that processes Personal Data must: limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements
No formal registration requirements apply.

10. Data Protection Officers
An organization must designate one or more individuals to be responsible for ensuring that the organization complies with the Manitoba PIPITPA.

11. International Data Transfers
Under the Manitoba PIPITPA, there are no formal restrictions on transfers of Personal Information from Canada to other jurisdictions. However, organizations are required to notify individuals if they use service providers outside Canada to collect and/or process Personal Information. As the definition of “service providers” is quite broad and includes affiliated entities, it is recommended that appropriate data transfer agreements be put in place to address the obligations of recipients of Personal Information in the context of onward transfers.
12. Security Requirements
An organization must protect Personal Information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

13. Special Rules for Outsourcing of Data Processing to Third Parties
An organization is responsible for Personal Data that is in its custody or under its control and where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person’s compliance.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
An organization is required to report incidents of security breach to an individual when the Personal Information about the individual that is under its control is stolen, lost or accessed in an unauthorized manner.

An organization that is involved in a data breach situation may be subject to: a suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions and/or class actions, and/or a criminal prosecution.

16. Accountability
There is currently no requirement for organisations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-blower hotline
Whistle-blower hotlines may be established in Canada provided that they are in compliance with local laws.

18. E-discovery
To the extent that Personal Information is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with the Manitoba PIPITPA. An organization should take privacy-related issues into consideration prior to the commencement and during the course of litigation.
Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization shall use contractual or other means to ensure that personal information and such system are protected while being processed by the third party.

19. Anti-Spam Filtering

Section 184(1) of the Criminal Code sets out the general rule that it is illegal to wilfully intercept a private communication, ‘Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.’

Therefore, the organization shall ensure that the introduction and the implementation of a spam-filtering solution is in compliance with the Manitoba PIPITPA (not yet in force) and the Criminal Code.

20. Cookies

There are specific laws/rules in Canada that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is generally required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent is not considered valid consent.
Ontario, Canada

1. Recent Privacy Developments

Ontario Courts Issue Additional Case Law on Tort of “Intrusion Upon Seclusion”

Ontario courts have continued to recognize and apply the tort of “intrusion upon seclusion”, which was first established by the Ontario Court of Appeal (“ONCA”) in 2012 as a right to bring a civil action for damages for the invasion of personal privacy.

In a decision released in July 2014, the ONCA held that a major bank could be vicariously liable for its employee’s commission of the tort of intrusion upon seclusion, and certified a class action against both the employee and the bank. The employee in question had confessed to accessing private and confidential information of the bank’s customers and providing it to his girlfriend who, in turn, disseminated the information to third parties for fraudulent and improper purposes. The case follows on an earlier decision of the Federal Court in March 2014, which certified a class action against the government for the tort of inclusion upon seclusion. The decision of the ONCA further extends the practical application of the tort to the context of vicarious liability.

In another decision released in October, the ONCA held that the plaintiff had established a factual basis for the tort of intrusion upon seclusion, but that the evidence presented did not support a claim for damages for the defendant’s improper access to the plaintiff’s private information. Nonetheless, the ONCA provided guidance on how such damages might be quantified. According to the ONCA, the following elements are required to establish a successful claim:

- The conduct must be intentional;
- There must be an “invasion” without lawful jurisdiction of a person’s private affairs or concerns; and
- A reasonable person would consider the event as highly offensive causing anguish, humiliation or distress.

The ONCA thereby confirmed the status of an intentional breach of privacy as an actionable claim that may lead to a damage award, in addition to any other damages, if substantiated by the evidence presented.
2. Emerging Privacy Issues and Trends

*Privacy Commissioner calls for change in the wake of health-related privacy class actions*

Following a number of high-profile privacy breaches and several class actions against Ontario hospitals, the Information and Privacy Commissioner of Ontario (“IPCO”) has called for an increased focus on privacy in the context of the provision of health care. In one case involving the sale of the Personal Information of thousands of patients by hospital staff, the IPCO commented that the hospital had failed to implement reasonable safeguards several months after the investigation. The IPCO has also publicly commented in favour of the development of a procedure to prosecute offenders, as well as legislative changes so as require hospitals to report privacy breaches to the IPCO on a mandatory basis.

*Spam* – Federal anti-spam legislation came into force on July 1, 2014, and the provisions thereunder that regulate the installation of computer programs came into force on January 15, 2015. For more information, see the summary of Canada’s Anti-Spam Legislation (“CASL”) in the Canada chapter.

3. Law Applicable


PHIPA establishes rules that govern the collection, use and disclosure of Personal Health Information regarding an individual (“Data Subject”) in order to protect the confidentiality of the information and the privacy of the Data Subject with respect to that information.

PHIPA applies to “health information custodians” when they collect, use or disclose Personal Health Information. Health information custodians are doctors, other health care practitioners, long-term care facilities, health care clinics, laboratories, pharmacies, the Ministry of Health and Long-Term Care as well as certain other health-related organizations. PHIPA also applies to organizations and individuals outside the health system when they receive Personal Health Information from an organization or an individual within the health system such as employers or insurance companies. It applies to everyone with respect to the collection, use or disclosure of health insurance plan numbers of Ontario residents.

4. Scope of the Law

a. Personal Data

“Personal Health Information” means identifying information with respect to a Data Subject in oral or recorded form whether the information relates to the physical or mental health of the Data Subject, including for example, information regarding the health history of the Data Subject’s family and the
provision of health care to the Data Subject. “Identifying information” means information that identifies a Data Subject or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify a Data Subject (“Personal Information” or “Personal Data”).

Personal Health Information does not include identifying information contained in a record that is in the custody or under the control of a health information custodian if either: (i) the identifying information contained in the record relates mostly to one or more employees or agents of the custodian; or (ii) the record is maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employees or other agents.

b. Data Processing

“Processing” is not expressly defined in PHIPA but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of the Data Controller, including handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating, deleting Personal Information – whether on a manual or automated basis. Further, a health information custodian may use Personal Health Information about a Data Subject for the purpose of obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health care or related goods and services.

c. Processing by Data Controllers

PHIPA governs the manner in which Personal Health Information is collected, used and disclosed within the health care system. It also regulates individuals and organizations that receive Personal Information from health care professionals.

d. Jurisdiction/Territoriality

PHIPA governs the Personal Health Information that is collected, used and disclosed in Ontario’s health care system. PIPEDA applies to all commercial activities relating to the exchange of Personal Health Information between provinces and territories and to information transfers outside of Canada. PIPEDA applies to federally regulated commercial organizations operating in Ontario.

Federal and provincial public sector privacy statutes apply to Personal Information in records held by government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.
e. **Sensitive Personal Data**
In determining the requisite form of consent to be obtained, organizations are required to take into account the sensitivity of the Personal Information. Personal Health Information is almost always considered sensitive therefore it should be treated in the manner described in Section 5 below.

f. **Employee Personal Data**
Personal Health Information does not include identifying information contained in a record that is in the custody or under the control of a health information custodian if: (i) the identifying information contained in the record relates primarily to one or more employees or other agents of the custodian; or (ii) the record is maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employees or other agents.

5. **Consent**
a. **General**
Generally, health information custodians must obtain a Data Subject’s consent to collect, use and disclose Personal Health Information unless an exception to this requirement applies. A Data Subject’s consent may be express or implied. A Data Subject may withdraw his or her consent at any time for the collection, use, or disclosure of his or her Personal Health Information by providing notice to the health information custodian.

    In accordance with PHIPA, consent is valid if it is knowledgeable, voluntary, related to the information in question and given by the Data Subject. In order to meet the criteria of knowledgeable, the Data Subject must know why a health information custodian collects, uses or discloses his or her Personal Health Information and that his or her may withhold or withdraw consent.

    A health information custodian is not required to obtain a Data Subject’s written or verbal consent each time Personal Health Information is used, disclosed or collected. PHIPA allows a custodian to assume implied consent where information is exchanged between custodians within the circle of care when providing direct health care unless the custodian has reason to believe that the Data Subject has expressly withdrawn or withhold their consent.

    Implied consent is also acceptable if a health information custodian collects, uses or discloses names or addresses for the purpose of fundraising. Also, if the Data Subject has provided information regarding his or her religious beliefs to the health care facility, the facility may rely on implied consent to disclose the Data Subject’s name and location within the facility to a person representing his or her religious organization in certain circumstances.
Express consent is required in the following circumstances and is subject to very few exceptions:

(i) where the Personal Health Information is disclosed to a Data Subject or organization, such as an insurance company if the organization is not a health information custodian; (ii) where information is disclosed from one custodian to another for a purpose other than providing or assisting in providing health care; and (iii) when a custodian:

- collects, uses or discloses Personal Health Information other than a Data Subject’s name and mailing address for the purposes of fundraising;
- collects Personal Information for marketing research or activities; and/or
- collects, uses or discloses Personal Information for research purposes, unless certain conditions are met.

When a Data Subject requests a health information custodian not to use or disclose his or her Personal Health Information to another custodian, the custodian must inform the recipient custodian that some Personal Health Information is inaccessible because it was “locked” by the Data Subject, if the custodian considers some of the locked information to be reasonably necessary for the provision of health care. However, a custodian may disclose the locked information in certain circumstances.

PHIPA generally presumes that Data Subjects are able to provide their consent to collection, use or disclosure of Personal Information when they are able to understand and appreciate the consequences of providing, withholding, or withdrawing consent. However, if a health information custodian is of the opinion that a Data Subject is not able to provide consent, PHIPA allows a substitute decision-maker to make a decision on behalf of the Data Subject.

b. Sensitive Data

An organization should seek express consent from a Data Subject when Personal Health Information is involved as health information is almost always considered sensitive. This is intended to ensure that the consent is given freely and is provided on an informed basis.

c. Minors

If the Data Subject is a child who is less than 16 years of age, a parent of the child or a children’s aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent may give consent on behalf of the child unless the information relates to (i) treatment within the meaning of the Health Care Consent Act, 1996, about which the child has made a decision on his or her own in accordance with that Act, or (ii) counselling in which the child has participated on his or her own under the Child and Family Services Act. If the Data Subject is a child who is less than 16 years of age and who is
capable of consenting to the collection, use or disclosure of the information and if there is a person who is entitled to act as the substitute decision-maker of the child as described above, a decision of the child to give, withhold or withdraw the consent or to provide the information prevails over a conflicting decision of that person.

d. Employee Consent
All the requirements set out by PHIPA for the giving of consent by any Data Subject shall equally apply to consent given by employees covered by PHIPA.

e. Online/Electronic Consent
Electronic consent will usually suffice if appropriate steps are taken to ensure a Data Subject is aware of the Data Controller’s data processing practices and policies (e.g., an appropriately accessible hyperlink, i.e., directly above a consent button).

6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

7. Processing Rules
An organization that processes Personal Data must: limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements
No formal registration requirements apply.
10. Data Protection Officers

A personal health information custodian must designate a contact person who is authorized to:

- facilitate the custodian’s compliance;
- ensure that all agents of the custodian are appropriately informed of their duties under this PHIPA;
- respond to inquiries from the public about the custodian’s information practices;
- respond to requests of an individual for access to or correction of a record of Personal Health Information about the individual that is in the custody or under the control of the custodian; and
- receive complaints from the public

Where the custodian is an individual (a natural person, not a company or an institution), the personal health custodian may act as the contact person.

11. International Data Transfers

Under PHIPA, the following restrictions apply in the case of transfers of Personal Health Information outside Ontario. A health information custodian may disclose Personal Health Information about a Data Subject collected in Ontario to a person outside Ontario only if:

(a) the Data Subject consents to the disclosure;
(b) PHIPA permits the disclosure;
(c) the person receiving the information performs functions comparable to the functions performed by a person to whom PHIPA would permit the custodian to disclose the information in certain prescribed circumstances;
(d) the following conditions are met: (i) the custodian is a prescribed entity in connection with planning the administration of the health system; (ii) the disclosure is for the purpose of health planning or health administration; (iii) the information relates to health care provided in Ontario to a person who is a resident of another province or territory in Canada; and (iv) the disclosure is made to the government of that province or territory;
(e) the disclosure is reasonably necessary for the provision of health care to the Data Subject, but not if the Data Subject has expressly instructed the custodian not to make the disclosure; or
(f) the disclosure is reasonably necessary for the administration of payments in connection with the provision of health care to the Data Subject or for contractual or legal requirements in that connection.
12. Security Requirements
An organization is required to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organizational security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and must comply with sector specific requirements.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
Subject to certain exceptions, a health information custodian that has custody or control of Personal Health Information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons.

An organization that is involved in a data breach situation may be subject to: a suspension of business operations, an administrative fine, penalty or sanction, civil actions and/or class actions, and/or a criminal prosecution.

16. Accountability
There is currently no requirement for organisations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-blower hotline
Whistle-blower hotlines may be established in Canada provided that they are in compliance with local laws.

18. E-discovery
To the extent that Personal Data is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with PHIPA. An organization should take privacy-related issues into consideration prior to the commencement and during the course of litigation.
Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization shall use contractual or other means to ensure that Personal Information and such system are protected while being processed by the third party.

19. Anti-Spam Filtering

Section 184(1) of the Criminal Code sets out the general rule that it is illegal to willfully intercept a private communication. ‘Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, willfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.’

Therefore, an organization should ensure that the introduction and the implementation of a spam-filtering solution is in compliance with PHIPA and the Criminal Code.

20. Cookies

There are specific laws/rules in Canada that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organisation that plans to engage in direct marketing activities with a Data Subject is generally required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organisation must obtain consent for a specific activity, as bundled consent is not considered valid consent.
Quebec, Canada

1. Recent Privacy Developments

Quebec Privacy Legislation Applies to Telecommunications Companies and Banks

A decision of the Commission d’accès à l’information (“CAI”) (the office of the provincial information and privacy commissioner in Quebec) has confirmed that Quebec’s private sector privacy legislation, An Act respecting the protection of personal information in the private sector (the “Quebec Act”), applies to telecommunications companies and banks in the province. Following a complaint against a major telecommunications company, the company made submissions in proceedings before the CAI without admitting the CAI’s jurisdiction over the matter. The company reasoned that telecommunications undertakings are an area of exclusive federal jurisdiction under the Canadian Constitution Act and that, as such, are only subject to the federal privacy legislation (PIPEDA). However, in its decision, the CAI reasoned that a telecommunications company carrying on an “organized economic activity” in the province falls within the meaning of an “enterprise” in the Civil Code of Quebec; as such, the telecommunications company fell within the scope of the Quebec Act, which applies to every person who “collects, holds, uses or communicates [personal information] to third persons in the course of carrying on an enterprise” in the province.

The CAI cited its own previous decisions and a 2014 decision of the Superior Court of Quebec in concluding that the Quebec Act applies to enterprises that fall under federal jurisdiction, which would include telecommunications companies and financial institutions. In order to exclude the application of the Quebec Act, a party would have to establish that such application has the effect of impairing the core of the federal power in question (e.g., telecommunications matters or banking). Moreover, as established in a decision of the Supreme Court of Canada cited by the CAI, where provincial and federal legislation may apply to the same situation and particularly where they have the same objective, an interpretation must be favoured that reconciles the two.

2. Emerging Privacy Issues and Trends

According to the CAI’s most recent annual management report, pamphlets and guidance documents, the following areas may be priorities for the CAI in the 2014-2018 period:

- Online behavioural advertising
- Informing the public about their access and other privacy rights
The application of privacy laws to landlord-tenant agreements

Ensuring proper destruction of records containing Personal Information

Spam – Federal anti-spam legislation came into force on July 1, 2014, and the provisions thereunder that regulate the installation of computer programs came into force on January 15, 2015. For more information, see the summary of Canada’s Anti-Spam Legislation (CASL) in the Canada chapter.

3. Law Applicable

An Act respecting the protection of personal information in the private sector, RSQ, c P-39 (“Quebec Act”).

4. Scope of the Law

a. Personal Data

Personal Information is any information which relates to a natural person (“Data Subject”) and allows that person to be identified (“Personal Information” or “Personal Data”). The Quebec Act applies to such information whatever the nature of its medium and whatever the form in which it is accessible, whether written, graphic, taped, filmed, computerized, or other. However, the Quebec Act does not apply to oral disclosures of Personal Information. The Personal Information must be in an accessible recorded form. The expression of an opinion about a Data Subject is a description of that Data Subject and, therefore, qualifies as his or her Personal Information. It is the nature of the information that characterizes it as Personal Information under the Quebec Act.

The Quebec Act, which has been in force since 1994, deals with the protection of Personal Information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise. The Quebec Act applies to both natural and legal persons carrying on an enterprise.

b. Data Processing

Processing is not expressly defined in the Quebec Act but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of the Data Controller, including the handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating, or deleting of Personal Information – whether on a manual or automated basis.

c. Processing by Data Controllers

A “file” (which is broadly defined as a group of organized data elements in some form of media – e.g., in writing, electronic media) may only be established when there is a serious and legitimate reason for doing so. The purpose/object of a file must be determined when the file is first established.
Personal Information for a file (described above) may be collected only as necessary for the object of the file.

A Data Controller cannot deny a Data Subject goods or services based only on the Data Subject’s refusal to disclose his or her Personal Information, unless:

- it is necessary for the conclusion or performance of a contract;
- it is authorized by law; or
- there are reasonable grounds to believe that the request is not lawful.

The Quebec Act expressly extends the foregoing prohibition to the employment context. An enterprise cannot refuse a Data Subject’s request for employment by reason only that the Data Subject has refused to disclose Personal Information, unless the information is necessary for determining whether the Data Subject is a suitable employment candidate.

d. Jurisdiction/Territoriality

All persons carrying on an enterprise in Quebec are subject to the Quebec Act, even if the enterprise’s head office is elsewhere. An enterprise cannot avoid the application of the Quebec Act by transferring files containing Personal Information collected, held and used in Quebec to a location outside the province.

The federal PIPEDA does not apply to those organizations in the province of Quebec that are subject to the Quebec Act with respect to their collection, use and disclosure of Personal Information within the province. PIPEDA applies to (i) federal works, undertakings and businesses in the province of Quebec and (ii) all transborder collections, uses and disclosures of Personal Information in the course of commercial activity.

Federal and provincial public sector privacy statutes apply to Personal Information in records held by government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.

e. Sensitive Personal Data

The Quebec Act does not include a definition of Sensitive Personal Information.

f. Employee Personal Data

The Quebec Act does not include a definition of Employee Personal Information.
5. Consent

a. General

Consent to the communication or use of Personal Information must be manifest, free, and enlightened, and must be given for a specific purpose. A consent that does not meet these requirements is without effect. A valid consent need not be in writing, but it must be precise and given for particular purposes. The Quebec Act prohibits the use of overly broad forms of consent. A new consent is required for each new purpose.

While the Quebec Act does not define “manifest, free and enlightened,” these terms suggest that consent must be evident, uncoerced and informed.

An enterprise must provide Data Subjects with an opportunity to opt out of using their Personal Information for internal marketing purposes.

b. Sensitive Data

An organization should seek express consent when Personal Information is likely to be considered sensitive, having regard to the reasonable expectations of the Data Subject. This is intended to ensure that the consent is given freely and is provided on an informed basis. The more sensitive the Personal Information is, the greater likelihood that express consent is required for its collection, use and disclosure.

c. Minors

The Quebec Act does not include any unique consent requirements applicable specifically to minors.

d. Employee Consent

The Commission d’accès à l’information (“Commission”) may, on written request and after consulting the professional orders concerned, grant a person authorization to receive communication of Personal Information on professionals regarding their professional activities, without the consent of the professionals concerned, if it has reasonable cause to believe:

- that the communication protects professional secrecy, especially in that it does not allow the identification of the person to whom the professional service is rendered, and does not otherwise invade the privacy of the professionals concerned;

- that the professionals concerned will be notified periodically of the intended uses and the ends contemplated and will be given a valid opportunity to refuse to allow such information to be preserved or to allow such information to be used for the intended uses or the ends contemplated; and
that security measures have been put into place to ensure the confidentiality of Personal Information. Such authorization shall be granted in writing. It may be revoked or suspended if the Commission has reasonable cause to believe that the authorized person is not complying with the above prescriptions, the intended uses or the ends contemplated.

The authorized person may communicate such Personal Information if:

- the information is communicated in a combined form that does not allow the identification of a specific professional act performed by a professional;
- the professionals concerned are periodically given a valid opportunity to refuse to be the subject of such a communication of information; and
- the person receiving communication of such information undertakes to use the information only for the intended uses and the ends contemplated.

e. Online/Electronic Consent

The Quebec Act does not include any provisions concerning written versus electronic consents. However, electronic consent will suffice if appropriate steps are taken to ensure a Data Subject is aware of the Data Controller’s data processing practices and policies (e.g., an appropriately accessible hyperlink, i.e., directly above a consent button).

6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the rights of the Data Subject; how the Personal Data is to be transferred; where the Personal Data is to be stored; how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

7. Processing Rules

An organization that processes Personal Data must: limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.
8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements
An organization that collects and processes Personal Data is not required to register, file and notify the appropriate data authority.

10. Data Protection Officers
Organizations may be required to designate a privacy officer or other individual(s) who will be responsible for the privacy practices of the organization.

11. International Data Transfers
An enterprise subject to the Quebec Act, which either communicates Personal Information outside Quebec about Quebec residents or gives a person outside Quebec the authority to hold, use or communicate the information on his or her behalf, is still accountable for that information and must take all reasonable steps to ensure that the information is not used for purposes irrelevant to the object of the file, nor communicated to third parties without consent of the Data Subject to whom the information relates.

12. Security Requirements
A person carrying on an enterprise must take the security measures necessary to ensure the protection of the Personal Data collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and must comply with sector specific requirements.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings and/or private rights of action.
15. Data Security Breach

There are no explicit security breach notification requirements in the Quebec Act. Nevertheless, an organization is generally required to take reasonable security measures to protect Personal Information under its control, and take appropriate action to address security breach situations that may arise, which action may include notification of Data Subjects, data authorities, and/or other parties.

An organization that is involved in a data breach situation may be subject to: a suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions and/or class actions, and/or a criminal prosecution.

16. Accountability

There is currently no requirement for organisations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of personal data.

17. Whistle-blower hotline

Whistle-blower hotlines may be established in Canada provided that they are in compliance with local laws.

18. E-discovery

To the extent that Personal Information is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with Quebec Act. An organization should take privacy related issues into consideration prior to the commencement and during the course of litigation.

Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization shall use contractual or other means to ensure that Personal Information and such system are protected while being processed by the third party.

19. Anti-Spam Filtering

Section 184(1) of the Criminal Code (Canada) ("Criminal Code") sets out the general rule that it is illegal to willfully intercept a private communication, ‘Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.’
Therefore, the organization shall ensure that the introduction and the implementation of a spam-filtering solution is in compliance with Quebec Act and the Criminal Code.

20. Cookies

There are specific laws/rules in Canada that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent is not considered valid consent.
Chile

Diego Ferrada
Santiago
Tel: +56 2 367 7087
diego.ferrada@bakermckenzie.com

Antonio Ortuzar Jr.
Santiago
Tel: +56 2 367 7078
antonio.ortuzar.jr@bakermckenzie.com
1. Recent Privacy Developments

The current government has rejected the idea of the “consolidated bill” and has presented for public comments an entirely new bill (the “New Bill”) which will wholly replace the current Personal Data Protection Act. The New Bill is supposed to be presented to Congress in the next few months.

The New Bill seeks to introduce the following main changes to the current Personal Data Protection Law:

a. A Data Protection Council will be created, which will be in charge of enforcing the Personal Data Protection Act and will have powers to impose important fines against violators.

b. The New Bill will impose fines for the first time, which are expected to reach USD 700,000.00.

c. In case of serious and repeated offences, a data controller will be prohibited from processing personal data.

d. The Law will incorporate most OECD personal data protection principles.

e. Data bases will have to register with the data protection authority.

f. There is also discussion about personal data of minors and personal data of deceased individuals.

2. Emerging Privacy Issues and Trends

With the New Bill, the Chilean government intends to bring the Chilean legislation to a higher standard.

3. Law Applicable


4. Key Privacy Concepts

a. **Personal Data**

“Personal Data” is defined as any information relating to identified or identifiable individuals.

b. **Data Processing**

Generally, Personal Data may be processed only when the Act or other legal provisions allow such processing or the Data Subject has expressly consented after being duly informed of the collection of its Personal Data and the purpose thereof.
c. **Processing by Data Controllers**

The Act does not provide for a data protection authority or require that private enterprises register Data Controllers or databases. The Act is a self-assessment compliance regime. It regulates the processing of Personal Data in databases (whether automated or not).

d. **Sensitive Personal Data**

“Sensitive Data” is defined as Personal Data that refers to the physical or moral characteristics of the Data Subject or to facts or circumstances of his private life such as personal habits, racial origin, political ideologies and opinions, religious beliefs, the status of his physical and mental health and his sexual life.

e. **Employee Personal Data**

With respect to employees, the law prohibits setting as a condition for hiring the absence of negative commercial information, or to require any statement or certificate on the same. The law exempts from this prohibition the case of hiring employees who will have the authority to represent their employer (managers, agents, etc.) and those who will work in collection, administration or custody of funds or securities.

5. **Consent**

a. **General**

Data Subjects should be informed about the purpose of the collection, processing and storage of Personal Data. According to the Act, the consent of the Data Subject should be voluntary, informed, and unambiguous, and must be in writing. There are some exceptions where no consent is required: (i) the Personal Data comes from sources available to the public; or, (ii) the Personal Data is processed for the exclusive use and general benefit of private legal entities, their members or affiliated entities, for statistical purposes, price setting or other purpose of general benefit. Personal Data should only be used for the purposes for which it was obtained.

b. **Sensitive Data**

Sensitive Data cannot be processed except when the Act allows for such processing; the Data Subject has given consent; or the Personal Data is necessary to determine or grant medical benefits that belong to the Data Subject.

c. **Minors**

There are no specific rules for minors.
d. **Employee Consent**

Section 4 of the Act unambiguously requires express written consent by the Data Subject for the processing of any Personal Data. If such Data Subject is an employee of the Data Controller/Data Processor, from a practical point of view, the easiest way to obtain consent from employees is to include a special clause in the standard format of employment agreements and the company’s Internal Regulations. This practice ensures that all employees will provide their consent prior to the data collection.

The Data Subject must have authorized the transmission of Personal Data. Authorization to collect and process Personal Data does not serve as authorization to transmit. Therefore, special language must be included in the authorization to collect and process authorizing the transmission of the Personal Data. Further, the general rule in the case of Sensitive Data is that a special authorization must be provided. To satisfy such requirement, it would be advisable to alert the Data Subject in the transmission authorization that Sensitive Data could be transmitted.

e. **Online/Electronic Consent**

Electronic consent is permissible and can be effective if properly structured and evidenced.

6. **Information/Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; third parties to which the organization will disclose the Personal Data; where the Personal Data is to be transferred; and the means of transmission of the Personal Data.

7. **Processing Rules**

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected.

8. **Rights of Individuals**

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. **Registration/Notification Requirements**

There are no requirements for organizations that collect and process Personal Data to register, file or notify the local data authority.
10. Data Protection Officers
There is no requirement for organizations to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers
The Act does not contain any special restrictions on the transfer of Personal Data to third countries. The new Bill (as discussed in Section 1) intends to establish territorial restrictions.

12. Security Requirements
The Act does not contain any specific security requirements.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Generally, the party responsible for the database will remain liable for the acts of the third party provider. The outsourcing services agreement must be in writing and must clearly indicate the scope of the services and liability of the third parties. Should the third party provider breach the contract, it may be subject to an independent liability under the Act.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, civil actions, class actions, or private rights of action.

15. Data Security Breach
There are no specific rules addressing data security breaches. Organizations that are involved in a data breach situation may be required to gather information about the breach; take steps to mitigate the harm to impacted Data Subjects; take steps to contain the breach and prevent future similar breaches; assist authorities with any investigation relating to the breach; and comply with court orders.

An organization that is involved in a data breach situation may be subject to civil actions and/or class actions.

16. Accountability
Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
There are no laws/rules regulating whistle-blower hotlines in Chile.
18. E-Discovery
When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of Personal Data is involved, and advise employees of the implementation of such system, the monitoring of work tools and the storage of Personal Data.

19. Anti-Spam Filtering
Generally, when a spam filtering solution is an automated process, it does not create privacy issues.

20. Cookies
The use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.
China

Nancy Leigh
Hong Kong
Tel: +852 2846 1787
nancy.leigh@bakermckenzie.com

Zhenyu Ruan
Shanghai
Tel: +86 21 6105 8577
zhenyu.ruan@bakermckenzie.com

Jacqueline Wong
Hong Kong
Tel: +851 2846 1563
jacqueline.wong@bakermckenzie.com

Howard Wu
Shanghai
Tel: +86 21 6105 8538
howard.wu@bakermckenzie.com

Tracy Zhang
Shanghai
Tel: +86 21 6105 8582
tracy.zhang@bakermckenzie.com
1. Recent Privacy Developments

*Consumer Protection Law Amended to Better Protect Consumer Data*

More comprehensive consumer rights, particularly with respect to personal data protection and additional responsibilities for online business operators, came into effect on 15 March 2014, with the amendment to the PRC *Consumer Protection Law*. The law significantly improves protection of consumer rights in their personal data (as further discussed below). Infringement of the law could lead to civil liability, fines of up to RMB 500,000.00 or in serious cases, the business could be shut down and its licence revoked.

*Supreme Court Provisions Confirm Tortious Liability for Privacy Infringement on Information Network*

The Supreme People’s Court issued the *Provisions on Several Issues concerning the Application of Law to Trial of Civil Disputes Concerning Infringement of Personal Rights over Information Networks*, effective from 10 October 2014 (“*SPC Provisions*”). The SPC Provisions stipulate that subject to prescribed justifications, Internet users or Internet service providers which publicize a natural person’s privacy or other personal information through information networks that cause harm to the individual shall be liable for tortious liabilities. Infringers may be ordered to offer an apology, eliminate negative influence or restore the reputation of the infringed person. They may be liable for compensatory damages if the infringed person suffered severe mental impairment or financial losses (the latter may include reasonable expenses incurred to cease the infringement such as legal fees).

*Regulations on Telecommunications and Internet User Personal Data Protection*

The Ministry of Industry and Information Technology (“MIIT”) promulgated the *Regulations on Telecommunications and Internet User Personal Data Protection* (“*MIIT Data Protection Regulations*”), which came into effect on 1 September 2013. The Regulations provide that telecommunications operators and Internet information service providers (“IISPs”) must comply with certain notification and handling requirements when collecting and using user personal data in the course of providing their services. The Regulations also stipulate storage and security requirements and require administrative authorities to investigate violations of the Regulations. Fines of up to RMB 30,000.00 may be imposed. IISPs include all companies with a PRC-based website, i.e., a site registered with or licensed by MIIT.
AQSIQ and SSC Released Guidelines on Personal Information Protection for Public and Commercial Service Providers

The General Administration of Quality Supervision, Inspection and Quarantine ("AQSIQ") and the State Standards Commission ("SSC") published the Information Security Technology - Guidelines for Personal Information Protection within Information System for Public and Commercial Services, which came into effect on 1 February 2013. The Guidelines set out the requirements regarding collection, processing, transfer and deletion of personal data. In particular, the Guidelines require data subject consent before transfer of personal data outside of China. The Guidelines only serve as a voluntary national standard (similar to a best practice standard) and its compliance is not mandatory.

Requirements on the Handling of Life Insurance Customer Information

The China Insurance Regulatory Commission ("CIRC") issued the Interim Measures for the Authenticity of Life Insurance Customer Information on 4 November 2013. The Interim Measures require life insurance companies and insurance brokers to restrict internal access to customer data, adopt measures to ensure security of customer data and to prevent data leakage, and prohibit disclosure and resale of customer data by the insurance salespersons.

Trial Measures for the Administration of Population Health Information

The National Health and Family Planning Commission promulgated the Trial Measures for the Administration of Population Health Information on 5 May 2014. “Population health information” is defined as “basic information of the population and medical and health services information, as generated by medical and health institutions of different types and at different levels in the process of their service provision and administration”. The Trial Measures require medical and health institutions to ensure information security of and protect personal privacy in the collection, utilization and management of population health information. In this connection, storing population health information in overseas servers, and hosting or leasing overseas servers, are prohibited under the Trial Measures.

New Regulations to Safeguard Security of Personal Information of Postal and Courier Service Users

The State Post Bureau issued the Provisions on Managing the Security of Personal Information of Postal and Courier Service Users on 26 March 2014. The Provisions require postal enterprises and courier service providers to adopt internal procedures and technical methods, as well as establish emergency response mechanisms, to manage user information collected in their service process. The Provisions prohibit disclosure of user information to third parties without legal authorization or user consent. In case of information...
leakage or loss, the responsible enterprise is required to take remedial measures and report to the post authority immediately.

**Draft Amendment to Criminal Law**

China is seeking better privacy protection by revamping its *Criminal Law*. The ninth draft amendment to the *Criminal Law* was released in November 2014 for public comment. Under the draft amendment, “selling or illegally providing personal information without consent of the information subject” is introduced as a criminal offence that carries a penalty of up to two years’ detention or imprisonment and/or fines. The crime of “misappropriating personal information obtained during the performance of duty or services” is currently limited to staff of government agencies and companies in certain industry sectors, and the draft amendment removes this limitation, resulting in a much wider scope of application. In addition, Internet service providers which persistently refuse to fulfill security management obligations causing serious leakage of user information could face criminal liability of up to three years’ imprisonment and/or fines.

2. Emerging Privacy Issues and Trends

The personal data protection provisions under the amended *Consumer Protection Law* and the various new regulations mentioned in Section 1 represent the continuing trend in China to regulate the collection and use of personal data.

The draft amendment to the *Criminal Law*, in the wake of massive data leakage incidents and misappropriation cases, reflects a growing consensus on the necessity of criminal law protection of privacy and personal information.

3. Law Applicable

While there is wide recognition in China for the need to protect privacy, there has yet been no specific legislation for the protection of personal data or privacy in China.

The *General Provisions of the Civil Code of the People’s Republic of China* (effective as of 1 January 1987) (the “Civil Code”), the *Opinion of the Supreme People’s Court on Several Problems in the Implementation of the Civil Code* (issued in 1988 and revised in 1990) and the *Answers of the Supreme People’s Court to Several Questions on Trying Cases Concerning Right to Reputation* (effective on August 7, 1993) (collectively the “Opinions”) address several issues relating to “privacy.”

This changed when the *Law of the People’s Republic of China on Tortious Liability* (the “Tortious Liability Law”) came into effect on 1 July 2010 and privacy rights were formally recognized as a form of civil rights and interests.
Under the current legal framework, the following laws and regulations are also relevant to privacy protection:

- the *Criminal Law*, as amended on and became effective on 28 February 2009;
- the *Decision on Strengthening the Protection of Network Information*, passed by the Standing Committee of the National People’s Congress on 28 December 2012 (the “NPC Decision”);
- the amended *Consumer Protection Law*, effective from 15 March 2014;
- industry-specific regulations governing telecommunications, banking, insurance, real estate brokerage, post and courier, health and other sectors (see Section 1 for examples).

4. Key Privacy Concepts
   
   a. **Personal Data**

   Neither the *Tortious Liability Law* nor the *Civil Code* or the *Opinions* refer to the term “personal data.” The Tortious Liability Law refers to “privacy rights” but gives no further elaboration on the scope of such privacy rights and/or the types of personal information that may be protected. The relevant term used in the Civil Code and the Opinions is “private affairs” of an individual. The term “private affairs” is not defined but potentially includes any type of personal information relating to individuals.

   Personal data in the cyberspace that is protected under the NPC Decision includes information in the Internet/networking environment that may identify an individual and/or relate to an individual’s privacy (“Electronic Personal Information”).

   Examples given by the Supreme People’s Court of privacy and personal information include genetic information, medical history, medical checkup records, criminal records, home address and private activities of a natural person.

   Following the amendments to the *Consumer Protection Law*, the State Administration for Industry and Commerce promulgated the *Measures for Punishments against Infringements of Consumer Rights and Interests*, which came into effect on 15 March 2015. The Measures define “consumer personal information” as “information collected by a business operator during the provision of goods or services that may, independently or in combination with other information, ascertain the identity of a consumer such as the consumer’s name, gender, occupation, date of birth, identity document number, residential address, contact details, income and financial position, health information, and consumption habits, etc.”
Industry-specific regulations typically set out their own definitions of “personal information” that is protected under the regulations. These definitions, while varying among different business sectors, generally cover the personal information of service users that are collected or possessed by service providers during or as a result of the service provision.

b. Data Processing

Under the *NPC Decision*, companies that, in their business operations, collect and use Electronic Personal Information:

- should only collect and use Electronic Personal Information where it is lawful, legitimate and necessary to do so;
- must explicitly inform the data subjects of the purposes, scope and manner of data collection and use, and must obtain the data subjects' consent to the same;
- must only collect and use the Electronic Personal Information in compliance with the law and as agreed with the data subjects;
- must keep the Electronic Personal Information collected strictly confidential, and must not disclose, tamper with, damage, sell or unlawfully provide the same to a third party;
- must adopt technical and other necessary measures to ensure that the data is secure, and must take remedial steps immediately where data disclosure, damage or loss occurs or may occur;
- must only send commercial electronic messages to a recipient’s email address, land line or mobile number with the recipient’s consent or at his/her request, or where the recipient has not expressly declined the receipt of the same.

There are very similar provisions under the amended *Consumer Protection Law* which impose the obligations on business operators that provide goods or services to PRC consumers.

Industry-specific regulations raise additional considerations with respect to data privacy in the relevant service sectors (e.g., telecommunications, insurance, post and courier, health, etc.). For instance, banking institutions in China must comply with the relevant rules issued by the China Banking Regulatory Commission in respect of cross-border transfer of personal data. Another example is that medical institutions in China are not allowed to store population health data (such as electronic medical records of patients) on servers located outside China.

A business operator is also advised to check the relevant industry-specific regulations and guidelines for specific requirements or recommendations on data processing.
c. **Processing by Data Controllers**

See Section 4(b) above. No distinction has been drawn between a data controller and any other user/processor of personal data.

d. **Jurisdiction/Territoriality**

None of the laws and regulations set out above have any extraterritorial effect.

e. **Sensitive Personal Data**

No such term is defined under the laws and regulations set out above. Under Chinese censorship rules, sensitive data is generally associated with prohibited data. Prohibited data generally includes data which may harm the interests of the State, cause social instability or infringe another person’s rights. In China, personal data relating to religious or other beliefs or political opinions may be regarded as prohibited data, the production, reproduction, access and dissemination of which is prohibited.

f. **Employee Personal Data**

The *Administrative Regulations for Employment Services and Employment* (effective as of 1 January 2008) (the “Employment Management Regulations”) use the term “personal data”, but this term is not further defined in the regulations.

Although there is no definition under Chinese law of “employee personal data,” general rules governing record retention of enterprises refer to special retention and local government/trade union consent requirements for documents and materials that arise from the operation and management of an enterprise whose preservation is of “value to the State, society and the enterprise.” Discussions with selected government officials indicate that such materials could include the personal data of employees, and it is recommended that local authorities be consulted regarding certain categories of data (e.g., health records, disciplinary action, pensions, social security information, etc.).

5. **Consent Requirements**

a. **General**

With the issuance of the NPC Decision, the consent of data subjects should be obtained for the collection and use of personal data in the cyberspace. Under the amended *Consumer Protection Law*, the collection and use of consumer personal data, and the sending of unsolicited commercial messages are subject to consumer consent.

b. **Sensitive Data**

No such term is defined under any of the laws and regulations set out above (but see Section 4(e)).
c. Minors

The Law of the PRC on the Protection of Minors (effective from 1 June 2007) provides that no person may disclose the private matters of PRC citizens under the age of 18. There is no guidance on the application of the requirements, however, and the general view is that the collection and lawful use of the personal data of minors with the consent of their parents or guardians is acceptable.

d. Employee Consent

Under the Employment Management Regulations, employers should keep their employees’ personal data confidential, and must obtain an employee’s written consent before publicizing his or her personal data.

In addition, if an employer has formulated a data processing policy, and such policy forms part of the employer’s company rules, the employer is required to consult the employees through the trade union, the employee representatives’ congress or other means.

e. Online/Electronic Consent

Electronic signatures are valid under PRC law, and data messages that can exhibit their contents in tangible form and can be retrieved, consulted and can reliably ensure that its contents have maintained their integrity without modification since its finalization shall be deemed to be a written document and an original document. Though PRC law provides that the use of a data message as evidence may not be refused solely on the grounds of its creation, sending, receipt or storage in electronic form, in practice, it is generally much more difficult to submit an electronic contract/data message as evidence as opposed to a hard copy signature.

6. Information/Notice Requirements

With the issuance of the NPC Decision, data subjects should be informed of the purpose, scope and manner of data collection and use of personal data.

Similarly, under the amended Consumer Protection Law, consumers should be informed of the purpose, scope and manner of the collection and use of their personal data.

The MIIT Data Protection Regulations require telecommunications operators and IISPs to advise users of the purpose, method and scope of the collection and use of their personal information, and the ways to inquire or correct information, as well as the consequences of refusal to provide such information.
7. Processing Rules

A business operator is advised to check the relevant industry-specific regulations and guidelines for specific rules or recommendations on data processing. Please also refer to Section 4(b) above and Section 13 below.

8. Rights of Individuals

Under the Tortious Liability Law, “civil rights and interests” of natural and legal persons are protected and the term “civil rights and interests” is broadly defined to include, among other things, the right to one’s name, reputation, honor, image and privacy. A person whose civil rights and interests have been infringed may demand that the infringer bear tortious liability by ceasing the perpetration of the act, returning property or restoring it to the original state, paying compensation for loss, making an apology and/or elimination of the effect and restoration of reputation.

Under the Criminal Law, it is a criminal offence for anyone who works in a government organization and companies in certain industry sectors to sell or illegally provide personal information obtained in the performance of duty or services, and for anyone who illegally obtains such personal information. Under the NPC Decision, the State protects electronic information that identifies an individual and/or relates to an individual’s privacy, and imposes certain obligations on organizations that collect and use such personal electronic information in their business operations.

As mentioned in Section 1 above, the amended Consumer Protection Law provides protection of consumer rights in their personal data.

9. Registration/Notification Requirements

No specific requirements for registration/notification with government authorities. However, if an information safety incident (such as a massive data leakage) occurs, the affected entity is generally required to report the incident to the industry regulator (see also Section 15 below).

10. Data Protection Officers

No specific requirements apply.

11. International Data Transfers

Transfers of personal data out of China are permitted so long as the consent of the data subject has been obtained and the effect of such transfer does not fall within any of the scenarios described in Section 4(e) above. Selected regulations suggest that local government authorities in charge of archives should be consulted before the implementation of international data transfers.

Certain sectors, however, are subject to specific restrictions. For example, according to rules issued by the People’s Bank of China, personal financial information collected within China must be stored, processed and analyzed in
China unless otherwise exempted. Similarly, medical and health institutions are prohibited from storing “population health information” on overseas servers (see Section 1 above).

12. Security Requirements

The *NPC Decision* requires that companies adopt technical and other necessary measures to ensure that the data collected is secure, and to take remedial steps immediately where data disclosure, damage or loss occurs or may occur. The amended *Consumer Protection Law* also imposes similar obligations on business operators that provide goods or services to PRC consumers.

Certain industry specific regulations contain detailed security requirements, for example, the State Post Bureau’s *Provisions on Managing the Security of Personal Information of Postal and Courier Service Users*.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

The consent of data subjects is required as the NPC Decision does not provide for any exemption for outsourcing arrangements. Certain sectors such as the financial sector may impose specific requirements.

14. Enforcement and Sanctions

Any infringement of privacy rights (as described in Section 4 above) will give rise to claims for injunctive relief and compensatory damages under the *Tortious Liability Law*.

Administrative penalties (e.g., issuing a warning, confiscating illegal income, imposing a fine, revoking the business license, etc.) may be imposed for violation of the privacy principles set out in the *NPC Decision*.

In serious cases, the above-mentioned activities may amount to a violation of the *Law of the PRC on the Imposition of Penalties in Connection of the Administration of Law and Order* (effective from 1 March 2006) (the “*Penalties Law*”). The Penalties Law is applicable to cases where the circumstances are not serious enough to amount to a crime but the administrative penalties are insufficient. Penalties imposed by the Public Security Bureaus under the *Penalties Law* include detention of up to 20 days.

Under the *Criminal Law* of the PRC:

- anyone who works in a government organization or a financial, telecommunications, transport, educational or medical institution and sells or unlawfully provides to a third party the personal information acquired in the course of providing the relevant services or fulfilling his or her duties shall be sentenced to three-year imprisonment or criminal detention and/or subject to a fine in serious cases;
• for those stealing or illegally obtaining the aforesaid information, the same sanctions will apply in serious cases; and

• if any of the above offenses is committed by an organization, it will be subject to a fine and all management and officers who are directly responsible will be subject to the sanctions stated above.

15. Data Security Breach
There is currently no “data protection authority” in China. None of the laws and regulations set out above specify any duty to notify data subjects.

That being the case, there are a number of “information safety/security” regulations, which were promulgated, not particularly for the protection of personal data, but more out of concern for preserving state secrets and preventing data loss and business disruption which are considered harmful to the “public interest” in general. In that regard, government organizations and sensitive industries are required to install security systems, take preventive measures, and when any “information safety/security incident” occurs, report in a timely manner to the authorities and take emergency measures.

“Information safety incidents” is a very broad concept, and generally covers all malicious attacks, equipment malfunctions or natural disasters which result in a massive breakdown of an information system and/or data loss or theft (it is a broader concept than that of “security breach”). These regulations do not include specific requirements for notifying the affected individuals, as they were drafted mainly from the perspective of state supervision and maintenance of order, instead of mitigating the impact on individuals.

In addition, there are industry specific regulations that impose special duties on certain types of data carriers, including telecommunications service providers as well as companies in the financial and securities industries.

Failure to comply with the notification requirements as discussed above may lead to investigations and queries from the relevant authority and ultimately result in the imposition of administrative penalties.

16. Accountability
An organization has no legal obligation to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-blower hotline
There are no laws/rules that govern whistle-blower hotlines in China.

18. E-discovery system
The implementation of an e-discovery system within an organization will not specifically raise any privacy issues in China.
19. Anti-Spam filter solution
The introduction of a spam-filtering solution in an organization will not raise privacy issues in China.

20. Cookies
There is no specific law/rule that governs the use and deployment of cookies in China.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.

Under the amended Consumer Protection Law, a business operator is prohibited from sending unsolicited commercial information to consumers who have not consented to receiving such information and who have expressly refused to receive the same.
Colombia

Sandra Castillo
Bogota
Tel: +57 1 644 9595 Ext. 2756
sandra.castillo@bakermckenzie.com

Carolina Pardo
Bogota
Tel: +57 1 644 9595 Ext. 2603
carolina.pardo@bakermckenzie.com
1. Recent Privacy Developments

National Database Registry

The Colombian Personal Data protection statute (“Law 1581”) created the National Register of Databases Registry (“NRDR”), which is a public list of databases operating in Colombia. According to Law 1581, the registration of databases will be administered by the Superintendency of Industry and Trade (“SIC”) and specifically by the Colombian Data Protection Authority (“DPA”).

On 13 May 2014, the Colombian government issued Decree 886 of 2014 (“Decree 886”), which regulates Article 25 of Law 1581 on the creation of the National Database Registry (“NDR”). The obligations under Decree 866 will not become effective until the DPA implements the NDR. For more details on this development and the current status of its implementation, please see Section 9 below.

Accountability Guidelines

The Deputy for the Protection of Personal Data at the Superintendence of Industry and Commerce (Colombian Data Protection Authority “DPA”), recently issued the document “Guidelines for the Implementation of the Accountability Principle” (hereinafter referred to as the “Guidelines”).

This document was issued by the DPA to help data controllers and processors of personal data of Colombian individuals implement within the organizations the accountability principle, which was introduced in the Colombian legislation through a chapter contained in Decree 1377 of 2013 (“Decree 1377”), secondary regulation of Colombia’s main data protection statute, Law 1581 of 2012 (“Law 1581”).

Articles 26 and 27 of Decree 1377 provide that data controllers in charge of the collection and processing of personal data of individuals who reside in the Colombian territory have the obligation to adopt the accountability principle in the processing of such data and must be capable of showing to the DPA that they have adopted effective and appropriate internal measures to comply with the obligations set forth in both Law 1581 and Decree 1377.

As per article 27, the internal measures adopted by data controllers must guarantee (i) that within the organization there is an administrative structure directly proportional to the structure and size of the data controller; (ii) that internal mechanisms are adopted to put into practice policies that include tools to implement and train personnel in the processing of data and in the policies related thereto; and (iii) to adopt procedures to attend to consultations and claims from data subjects.

The Guidelines are aimed at explaining and detailing to data controllers the specific measures that can be adopted by them to comply with the obligation contained in Decree 1377. It is worth highlighting that as indicative of its
name, the Guidelines are a guiding tool for data controllers in complying with the obligation, but are not mandatory.

Nevertheless, the DPA has highlighted what Decree 1377 provided in relation to the implementation of the accountability principle and it is that all organizations that undertake the commitment to protect personal data adopting the measures detailed in the Guidelines or equivalent measures applying the accountability principle, will be treated with preferential leniency in the graduation and imposition of fines for lack of fulfillment of the obligations contained in Law 1581 and Decree 1377. This is particularly relevant as the DPA has recognized that it has limited resources to pursue every single infringement of the personal data protection laws and therefore, if a data controller is able to demonstrate that it has adopted the measures similar or identical to those described in the Guidelines and that the infringement was isolated, the DPA may decide to even refrain from opening an investigation.

Some of the highlights of what the Guidelines have defined as an Integral Personal Data Management Program (hereinafter referred to as the “Program”) aimed at applying the accountability principle, are the following:

- **Involvement of the company’s top management in developing, implementing and verifying compliance of and adequate adoption by all areas of the company.**

- **The appointed area or person within the company with data protection officer duties (having this person or area is mandatory as per article 23 of Decree 1377), must, among other duties:**
  - Actively contribute in the development and implementation of the Program and the drafting of policies for the processing of personal data;
  - Develop a personal data risk assessment system;
  - Be the liaison between top management and all areas of the company for data processing and any projects that entail processing of personal data;
  - Promote a culture of personal data protection within the company;
  - Keep an inventory of all databases of the company that contain personal data;
  - Record the recordal of databases with the DPA once the National Database Registry is implemented;
  - Process and obtain the corresponding declarations of conformity with the DPA for specific data processing and sharing projects;
  - Review, amend and approve data transmission agreements;
o Conduct internal trainings related to the effective compliance with the System and with the internal policies adopted by the company to effectively and lawfully process personal data.

o Attend and respond within the standards adopted by the System and the time frames provided for in Law 1581 to claims and consultations made by data subjects regarding the processing of their personal data.

o Actively cooperate with the DPA whenever said entity opens an investigation to the company or makes any information request regarding the processing of personal data by the company.

• Internal report and auditing mechanisms for data processing and management.

• Effective control systems for compliance of the System and policies for the processing of personal data.

• Effective administrative and operation protocols.

• Adequate database inventory

• Adoption of data processing policies and manuals consistent with the content requirements of Decree 1377 and with the realities of the company’s data flows.

• Adoption of privacy impact assessment mechanisms that have the following phases: i) identification; ii) measurement; iii) control; and iv) monitoring.

• Robust internal training programs for all employees to guarantee knowledge, awareness and compliance with the law, the System and the company’s internal policies and procedures.

• Adopt a robust methodology to receive and attend claims and consultations from data subjects.

• Adequately manage the relationship with data processors and the cross-border circulation of data in the way in which they handle, process and circulate personal data, which includes having robust contracts with them regulating the circulation of data in compliance with Law 1581 and Decree 1377.

• Appropriate communication strategies of internal and external data subjects to be duly informed and become aware of their rights, how to exercise them and the company’s policies in relation to the processing of personal data.
Periodical supervision, evaluation and assessment of effective compliance of the law and the System.

The Guidelines extensively comment and develop all of the above mentioned recommendations and we highlight and applaud the effort that the Colombian DPA has put into developing a clear and informative document that will become a very useful tool for data controllers to understand the implications that handling personal data has.

2. Emerging Privacy Issues and Trends

Some of the highlights of Decree 1377 include the following:

- The Decree introduces the concept of “transmission” which differs from that of “transfer”. The transfer of Personal Data requires prior, express and informed consent of the Data Subject (unless said transfer is subject to the exceptions provided by Law 1581). On the other hand, transmission is understood as the movement of Personal Data from Data Controllers to Data Processors. Transmissions will no longer require prior and informed consent of the Data Subjects if the Data Controller and the Data Processor enter into a transmission agreement. Furthermore, the transmission will be upheld if the parties sharing the data have all adhered to the same privacy policy accepted by the Data Subjects.

- The Decree also develops the concept of “prior, express and informed consent”- See Section 5(a).

- Processing of Personal Data of minors- See Section 5(c).

- The Decree introduces the concepts of “privacy policy” and “privacy notice”- See Section 6.

- Obligation of Data Controllers and Data Processors to appoint a Data Protection Officer- See Section 10.

- Data breach obligations - See Section 15.

- Introduction of the accountability principle- See Section 16.

- Do not call approaches and developments- See Section 21.

3. Law Applicable and Data Protection Authorities

a. Law Applicable

The Colombian Constitution introduced the fundamental right to habeas data, which is the right that every person has to self-determine the collection, use, storage, processing and transfer of his or her Personal Data, granting it special protection.
The Constitution mandates that the protection of fundamental rights must be detailed and ratified by one or more Statutory Laws. Statutory Laws require absolute majorities and a special proceeding within the Colombian Congress to be approved and must be signed into law by the President before they come into force.

In Colombia, the protection of the habeas data right is currently based on the provisions of the Constitution, and the following laws that regulate the right:

- Statutory Law 1581, which regulates privacy rights in respect of Personal Data collected and processed in any type of database, ("Law 1581").
- Statutory Law 1266, which regulates data privacy rights related to commercial and financial data for credit rating purposes, ("Law 1266").
- Statutory Law 1273 of 2009, which provides that certain actions undertaken in managing and processing Personal Data are inappropriate and qualify as felonies under the Colombian Criminal Code ("Law 1273").

The abovementioned statutes have been subject to interpretation by the Constitutional Court (the “Constitutional Rulings”). These Constitutional Rulings should be referred to in clarifying and understanding the context and rights under the relevant statutes.

Although data protection rules are generally applicable across all databases, the SIC, the Ministry of Communications and Information Technology and the Ministry of Commerce, Industry and Tourism, issued a supplementary regulation through Decree 1377 of 2013, to develop further specific issues already covered by Law 1581 and more recently, Decree 866 of 2014 in relation to the National Database Registry.

4. Key Privacy Concepts

a. Personal Data

Law 1266 regulates the collection, processing, storage, transfer and use of Personal Data related to credit rating activities. This Law defines Personal Data as any piece of information linked to one or more identifiable individuals or legal entities or to information which may be associated with a certain individual or legal entity.

Under Law 1266, Personal Data is classified into three different categories: (i) private data, which has a reserved and intimate nature that concerns a Data Subject; (ii) semi-private data is data that refers to an individual or person and is required by third parties (e.g., financial entities) to make certain assessments with respect to a person; and (iii) public data, which refers to information of a determined person, that has been validly recorded in public registries, judicial rulings or public documents, and all other data that are not private or semi-private in nature.
On the other hand, Law 1581 provides for a general framework related to the protection of data privacy rights. Hence, this Law regulates the collection, processing, storage, transfer and use of Personal Data, when such treatment occurs in any database in Colombia or with respect to Data Subjects domiciled in Colombia, where such data is susceptible to treatment by public or private entities.

Law 1581 only applies to individuals. According to the Constitutional Ruling of 2011, Law 1581 could apply to the protection of data privacy rights of legal entities when there is an infringement to the rights of individuals who are part of such entity.

For the purpose of this document, “Personal Data” and “Data Subject” should be understood as defined in Law 1581, unless otherwise stated or when specifically making reference to Law 1266.

According to the Rulings of the Constitutional Court referring to Law 1581 and Law 1266, the right of a person to authorize the processing of his Personal Data is not transferable. However, Law 1581 makes reference to some cases where a legal representative or a third party representing the Data Subject can validly grant consent. This is the case, for example, when the life or health of the Data Subject is at risk.

b. Data Processing

Law 1581 defines Data Controller as “an individual or legal entity, public or private, that either alone or in association with others, decides over the data base and/or on processing of the data” and Data Processor as “an individual or legal entity, public or private, that either alone or in association with others, processes Personal Data on behalf of the data controller”. Any processing of Personal Data governed under Law 1581 has to be done in accordance with the obligations that Data Controllers and Data Processors have under said Law.

According to the Constitutional Ruling of 2011, Law 1581 is applicable to residents in the territory of Colombia. It is also applicable to processing that takes place outside of Colombia but in relation to residents within the Colombian territory. This is specially relevant to cloud computing and online processing of Personal Data.

c. Processing by Data Controllers

A Data Controller or information operator can only process Personal Data within the scope of the prior, express and informed Consent granted by the Data Subject, unless one of the exceptions established in Law 1581 or in Law 1266 applies.

According to Law 1266, prior, express and informed Consent is required to report credit history of individuals and legal entities to financial databases. The databases are subject to registration and rules relating to the management of
the data and the publication of reports regarding such credit history. Failure to abide by such rules, triggers fines and sanctions.

According to Law 1581, prior and informed Consent of the Data Subject will be required except for the following circumstances:

- when the processing is authorized by a Law for historic, statistical, scientific, or other purposes;
- when the information is of a public nature;
- when the information is required by a government authority exercising its duties, as explicitly conferred by law;
- when the circulation of Personal Information is necessary in the event of a medical or sanitary emergency; and
- information regarding the civil registry.

d. Jurisdiction/Territoriality

Law 1266 applies equally to individuals and legal entities, in connection with data privacy rights related to credit rating activities in Colombia or related to Colombian persons.

Law 1581 establishes that its provisions are applicable to Data Subjects in the following cases:

- All data processing carried out in Colombia.
- All data processing carried out abroad but performed by a Data Processor or Data Controller whose acts are ruled by Colombian provisions according to international treaties. This means that activities of a Data Processor or a Data Controller that refer to individuals domiciled in Colombia, are subject to the provisions of Law 1581.

e. Sensitive Personal Data

The concept of Sensitive Personal Data includes, but is not limited to, any racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual preferences or habits and behavior. In general, Law 1581 defines Sensitive Personal Data as that which can affect the privacy of the Data Subject or the misuse of which can lead to discrimination.

f. Employee Personal Data

Employees’ Personal Data is likely to include Sensitive Personal Data (e.g., health-related information) and non-sensitive Personal Data.

Employees’ Sensitive Personal Data should be processed in accordance with the applicable laws mentioned in Section 4(e) and the Constitutional Rulings.
5. Consent

a. General

Under Law 1581, any collection, use, transfer, storage and processing of Personal Data requires prior, express and informed Consent from the Data Subject, except as provided for in Section 4(c).

In the Constitutional Ruling of 2011, the Court stated that consent can be granted through a “specific indication”. Hence it is possible to consider that an affirmative action will be construed as express consent, and thus if the elements of a prior and informed authorization from a Data Subject are also met, this should amount to adequate consent. In many Constitutional Rulings and also in the Constitutional Ruling of 2011, the Court has confirmed that silence, tacit consent and blanket consents are not acceptable.

Data Subjects have the right to revoke or request the suppression of their Personal Data at any time, except for certain instances in which the Data Controller must preserve the Personal Data (i.e., fraud prevention, etc.)

b. Sensitive Data

Law 1581 specifically establishes that processing of Sensitive Personal Data is unlawful unless the Data Subject has given his or her explicit consent or the processing is within the following exceptions:

- Processing is necessary to protect the life and health of the Data Subject and he or she is not legally or physically able to express his or her consent; In these cases, their representative must grant the authorization;
- If the processing corresponds to legitimate activities carried out with the appropriate guarantees by foundations, NGOs, associations or any other non-profit organization with a political, philosophical, religious or trade union purpose, if such data processing is only related to the members of the association or persons with whom the association is in recurrent contact because of its objective. In these events, the data may not be provided to third parties without the permission of the Data Subject;
- Processing refers to data that is necessary for the recognition, exercise or defense of a right under a judicial proceeding and;
- The processing has a historical, statistical or scientific purpose. In this event, measures must be taken for suppression of the Data Subject can be identified.

c. Minors

Minors are children and adolescents under the age of 18. In the Constitutional Ruling of 2011, the Court brought up the definition of minor from the Code of Infancy and Adolescents, indicating that for purposes of Law 1581, children
are individuals between 0 and 12 years old and adolescents are individuals between 12 and 18 years old.

However, the Constitutional Ruling of 2011, established that the prohibition of the processing of data of Minors does not apply when such processing of data guarantees that the fundamental rights of Children and Adolescents will be safeguarded, which implies that any processing of Personal Data of Minors should strictly comply with the Constitution and Law 1581, and other provisions as applicable.

Although Law 1581 does not contemplate explicitly the need for the consent from minors, the Constitutional Ruling of 2011 has included some guidelines that must be followed for the processing of minors’ Personal Data to be lawful: (i) the treatment shall respond to and comply with the highest interests of the children and adolescents; (ii) it shall be compliant with the minors’ constitutional rights; and (iii) as far as possible, the treatment shall be made taking into account the opinion of the minor to whom the Personal Data refers, in consideration of their maturity, autonomy and capacity to understand the situation referred to such processing of their Personal Data and the consequences that this entails. The evaluation of these factors must be made on a case by case basis. These guidelines inspired Article 12 of Decree 1377 and therefore, they are no longer mere guidelines but current regulation that must be followed whenever the processing of data of minors is required.

d. Employee Consent

Law 1581 and Decree 1377 do not provide for a specific provision on the requirements to implement monitoring mechanisms on employees (i.e., through their computers, surveillance cameras, telephones and cellphones, among others). However, multiple Constitutional rulings have established that the employer should seek prior, express and informed consent from employees to collect and process their Personal Data through such monitoring devices, even though the devices belong to the company.

In addition, in Colombia, employee consent is required when implementing a “Bring Your Own Device” (“BYOD”) program in the workplace.

e. Online/Electronic Consent

Consent can be obtained electronically since electronic contracts are valid and binding in Colombia. The foregoing is based on the rules established in Law 527 of 1999 (“Law 527”), which indicate that unless otherwise required by law, the parties are free to enter into any contract by any means and express their will to bind themselves in any way they choose and to the extent permitted by law. Electronic messages have the same legal effects as written documents and therefore in principle they can replace the requirement of the written document as per Law 527.
6. Information/Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to contact the privacy officer or other person accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

Decree 1377 introduces the concept of a “privacy policy” and the obligation of its implementation by Data Controllers. It also specifies the content required to appear in the said policy. In addition, Decree 1377 states that a “privacy notice”, which contains the organization’s “privacy policy”, should be made available especially in cases where information of said policy cannot be provided to the Data Subject. In any case, the privacy notice must contain a link or a reference indicating where to access and consult the privacy policy. Decree 1377 provides a description of the information that the privacy notice must contain.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met. One of the obligations that Data Controllers and Processors have is to adopt an internal manual of policies and procedures that are followed to guarantee that the provisions contained in Law 1581 and its applicable regulations, are effectively followed.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. Registration/Notification Requirements

Law 1581 created the National Database Registry (“NDR”), which is a public list of databases operating in Colombia. The registration of the databases will be administered by the SIC and specifically by the DPA.
On May 13, 2014, the Colombian government issued Decree 886 of 2014 ("Decree 886"), which regulates Article 25 of Law 1581 on the creation of the National Database Registry ("NDR").

Decree 886 extensively regulates the obligation that Data Controllers have under Article 25 of Law 1581 of 2012 to record with the NDR, information on certain characteristics of their databases containing personal data and which processing is subject to Colombian laws.

This obligation will not become effective until the Colombian DPA implements the NDR. In February 2015, the DPA officers published for public comments an implementation regulation of the NDR, along with the draft of the proposed manual of the NDR, after which tests and trials will be conducted to confirm the stability of the system. Thus, we anticipate that the NDR will be fully implemented around or before mid-2015.

Once the NDR is implemented by the SIC and in accordance with the provisions of Decree 886, Data Controllers will have the obligation to record certain information pertaining their databases. The main highlights of this new regulation include:

- **One year recordal deadline for databases created before the implementation of the NDR.** Data controllers will have to record their databases created before the official implementation date of the NDR, within one year counted as of the official implementation date of the NDR.

- **Two months recordal deadline for databases created after the implementation of the NDR.** Data controllers will have to record their databases created after the official implementation date of the NDR, within two months counted as of the creation of the corresponding database.

- **No recordal of the database itself.** Decree 886 does not require the recordal of the database itself. The purpose of the NDR is more focused on informing Data Subjects and the SIC of the databases that Data Controllers have and the conditions in which Data Controllers process Personal Data.

- **Separate filings must be made per database.** Data Controllers will have to make separate filings with the NDR for each database in which they hold Personal Data that they collect and process.

- **Database information that must be recorded with the NDR.** For each database that is recorded with the NDR, Decree 866 requires specific information and documentation to be detailed and uploaded.
10. Data Protection Officers

Organizations are required to designate a privacy officer or individual who will be responsible for the privacy practices of the organization. The duties of this officer can be exercised either by a specific individual or by an area or division within the organization. While Colombian laws do not require the privacy officer to be located in Colombia, such privacy officer is obliged to respond in a timely manner to all queries and complaints in Spanish, and must be fully knowledgeable of the organization’s operations and privacy policies.

11. International Data Transfers

The general rules established by Law 1266/08 and the Constitutional Court require that any transfer of private or semi-private Personal Data should be previously authorized by the Data Subject. Personal Data that originates from a foreign country does not require the Data Subject’s prior Consent.

Law 1581 prohibits the transfer of any Personal Data to countries that do not provide adequate levels of protection. Law 1581 provides that there is an adequate level of protection if the regulations of said country meet the standards set by the SIC on the subject, which in no case can be lower than the standards established by Law 1581.

The prohibition for the international transfer of Personal Data has the following exceptions, as described in Law 1581: (i) prior authorization from the Data Subject; (ii) exchange of medical information for reasons of health and public hygiene; (iii) exchange of financial information in connection with transfers or banking operations, according to the applicable legislation; (iv) transfer of data in compliance with an international treaty which Colombia is a party to; (v) necessary transfer of Personal Data for the execution of a contract between the Data Subject and the Data Controller; and (vi) transfers of data legally required to protect the public interest.

The Constitutional Ruling of 2011 provided some guidelines on the international transfer of Personal Data.

Law 1581 gave the Colombian Government the authority to issue: a supplementary regulation on binding corporate rules (“BCRs”); the certification of good practices in data protection; and a list of countries with adequate levels of protection for the cross-border transfer of Personal Data.

To date, the Colombian government has not yet issued a list of countries that are deemed to have adequate levels of protection. Nor has it issued a regulation governing BCRs. In effect, even if an organization has BCRs in place, they are not deemed useful for purposes of international transfers of data, where processing of data is subject to Colombian laws.
12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and are required to comply with sector specific requirements. Organizations shall be liable together with third party providers in case of breach by the latter.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, criminal proceedings, and/or private rights of action. Sanctions and penalties will be subject to reduction if data controllers and processors apply the accountability guidelines on which the SIC is currently working.

15. Data Security Breach
Pursuant to Law 1581, both Data Controllers and Data Processors have the duty to notify the Data Deputy of any breach to security codes and risks in the management of Data Subjects’ Personal Data, regardless of the nature and scope of the breach.

There is no obligation under Law 1581 to report the security breach to the Data Subject. However, the accountability principle guidelines on which the government is currently working on, include a recommendation on notifying Data Subjects, which is deemed by the SIC as an advisable practice that will be seen in a favorable light in case any investigations are initiated pursuant to a data breach report.

An organization that is involved in a data breach situation may be subject to a suspension of business operations; closure or cancellation of the file, register or database; administrative fine, penalty or sanction; civil actions and/or class actions, or a criminal prosecution.

16. Accountability
Data Controllers must be capable to demonstrate to the Colombian data protection authorities that they are in compliance with the measures included in the Decree and with the obligations established in Law 1581.
Subject to regulatory guidelines, which are currently being drafted by the SIC and have already been subject to discussion with select organizations that have shown interest in working with the SIC in developing guidance and regulations that ease the compliance of the existing laws and regulations, organizations may be required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data; furnish the results of the privacy impact assessments to the privacy regulators upon request; and furnish evidence relating to the effectiveness of the organization’s privacy management programme to privacy regulators upon request.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Colombia as long as they are in compliance with local laws.

18. E-Discovery

The process by which electronically-stored information is reviewed, processed and presented for the purposes of litigation or regulatory requests is valid under Colombian law. Electronic information can be stored in databases as structured content, in emails or instant messages as semi-structured content, and in documents or files as unstructured content. Nevertheless, employers should advise employees of the implementation of an e-discovery system and also that the use of work tools (e.g., e-mail, Internet) is being monitored and information such as e-mails will be stored. Nevertheless, employees may request the employer to destroy any Private Information stored as a consequence of the implementation of the e-discovery system. The employer may justify his position by alleging that such information is crucial for complying with regulations and/or for purposes of litigation.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.

20. Cookies

There are no specific laws/rules in Colombia that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used.
21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject's failure to respond. Opt-out consent is permissible. Consent of the Data Subject must be obtained for a specific activity. Bundled consent is not considered valid consent.

The Communications Regulation Commission ("CRC", a special government agency) has developed the Excluded Numbers Registry, in which consumers can sign up their mobile numbers to stop receiving advertising text messages. This registry was created by Resolution No. 2229 of 2009. Despite this specific regulation, Law 1581 requires the Data Subjects' prior, express and informed consent when any contact is made for advertising purposes; otherwise, such contact would be deemed as illegal.
Croatia

Luka Tadić-Čolić
Zagreb
Tel: +1 385 1 4925 488
luka.tadic@wolftheiss.com
1. Recent Privacy Developments

The key legislation regulating data protection in Croatia is the Data Protection Act (“Act”). The Act came into force in 2003 and to date has been amended three times: in 2006, 2008 and 2011, respectively. As of the 2011 amendments, the Act has been fully harmonized with EU data protection legislation (most notably with EU Directive 95/46/EC on Protection of individuals with regard to the processing of personal data and on the free movement of such data (“Directive”).

Supervision of data protection compliance in Croatia is entrusted to the Croatian Data Protection Agency (“DPA”). In addition, the DPA maintains the relevant data protection registers, provides guidance on a range of data protection matters and decides on data protection violations.

To date, the DPA has not published any consolidated guidance, list of principles or similar document that would list their practices and recommendations with respect to data protection matters in Croatia. This lack of regulation has two immediate consequences.

Firstly, EU soft law (including communications, working papers, decisions and other available materials) represents a principal interpretative tool in all data protection matters in Croatia in which the DPA has not already decided and taken a standpoint.

Secondly, a number of emerging data protection issues (such as privacy aspects of cloud computing and specific issues of cybersecurity, regulation of big data industry) remain, to a considerable degree, in a state of constant flux, without definitive guidelines as to what businesses and organizations can and cannot do.

However, despite this lack of legislative initiative by the DPA, the last few years have been very exciting times for all data protection practitioners in Croatia. The DPA has put considerable efforts into implementing and maintaining an effective and coherent data protection country-wide policy, and the results are beginning to show. For example, in the last two years the number of administrative acts issued by the DPA is believed to have increased by approximately 200%.

New important directions for data protection in Croatia will most likely come from the EU and be related to the new, much debated European Commission proposals on data protection reform.

2. Emerging Privacy Issues and Trends

The DPA recently published its Action Plan for 2015 – 2017. The main focus of the plan is to increase data protection enforcement.
The DPA plans to expand its efforts in improving the operational part of its enforcement and monitoring activities. Having in mind continuous technology developments (which almost as a rule comes in Croatia through users, and not developers who would ensure compliance with local laws from early on), the regulator plans to allocate more significant resources to educate local businesses and individuals on the importance of data protection compliance.

Besides the plan, the DPA also recently initiated and engaged in a debate on the following data protection matters:

- **Social Media.** In the last year, the DPA has, on several occasions, dealt with the issue of privacy in social media. This especially concerned protection of the privacy of minors, in relation to the content they upload online.

- **Employee Monitoring.** The DPA recently issued an opinion on monitoring at the workplace, finally drawing a clear line on what types of monitoring are permitted by employers and under which circumstances. The opinion relies on established EU standpoints on this issue.

- **Cookie Consent Requirement.** Croatian legislation has fully adopted EC e-Privacy Directive and opted for the so-called “opt-in” approach with respect to cookies. For details, see Section 20.

- **Online Direct Marketing.** Online direct marketing is generally allowed in Croatia as long as the individual is informed that his/her personal data will be used for marketing purposes and that he/she has the right to deny the consent for such use. For details, see Section 21.

- **Cybercrime/Cybersecurity.** Cybersecurity is becoming more and more important in Croatia. In the past year, identity thefts and “false enforcements”, using stolen or otherwise illegally procured personal tax numbers of Croatian citizens, have increased significantly. The problem is particularly complex as in many cases, citizens voluntarily give their tax numbers in job applications, promotional offers and similar cases. The DPA also recently organized a series of events dealing with this issue.

### 3. Law Applicable


Apart from the Act, specific aspects of data protection are regulated in sector-specific statutes, such as Labour Act (employment-related aspects of data protection and processes), Patient Rights Protection Act (privacy of patient data) or the Electronic Communications Act (use of cookies).
As Croatian data protection legislation is fully harmonized with the EU data protection rules, communications, working papers and the jurisprudence of the EU data protection bodies are regularly used as interpretative tools in all cases when local rules are silent on certain issues.

4. Key Privacy Concepts

In light of the harmonization of EU data protection legislation with the Croatian data protection rules, Croatian privacy concepts are almost, without exception, identical to the ones set out by the Directive.

a. Personal Data

The Act provides a rather broad definition of personal data describing it as any information pertaining to an identified individual or an identifiable individual (i.e., the one who can be identified, directly or indirectly, particularly on the basis of an identification number or one or more factors specific to the person’s physical, physiological, mental, economic, cultural or social identity).

Therefore, personal data would constitute any information that can be used to identify or profile a particular individual. Specific examples of personal data include an email address, bank account number, school records, filled out questionnaires, a photo and other data.

b. Data Processing

The Act adopts the same definition of data processing as the Directive, defining it as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making it otherwise available, alignment or combination, blocking, erasure or destruction.

However, under the Act, data processing also includes performing logical, mathematical and other operations on such data.

c. Processing by Data Controllers

A data controller is an individual or an entity which determines the purpose and means of data processing.

Although the Act allows personal data to also be processed by data processors (based on a contract with data controllers), the data controller’s responsibilities are considerably wider than those of data processors and include ensuring that the data is collected and disposed of in a legal and appropriate manner, in accordance with the Act and other applicable legislation.

For details on processing rules in Croatia, see Section 7.
d. Jurisdiction/Territoriality

The Act applies to the collection and processing of personal data of all individuals on the territory of the Republic of Croatia, regardless of their citizenship or place of residence or any other factors.

This also applies even if the data controller does not have its residence or seat in one of the Member States, and uses equipment for personal data processing which is located in the Republic of Croatia (except when such equipment is used solely for the transfer of personal data through European Union territory).

The Act does not apply to the processing of personal data conducted by individuals exclusively for personal or private purposes.

e. Sensitive Personal Data

The Act differentiates between sensitive personal data and non-sensitive personal data.

Sensitive personal data is any personal data pertaining to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health or sexual orientation, as well as personal data regarding criminal and misdemeanour proceedings.

Under the Act, sensitive data may be collected and subsequently processed only if all of the following three conditions are met:

A. one of the following grounds for collection and processing of sensitive data has been met:

   o where the relevant individual consents to such processing;
   
   o if the processing is necessary to exercise the rights and obligations of the data controller based on special regulations;
   
   o if the processing is necessary for the protection of life or physical integrity of another person, when the individual is unable to provide his/her consent to such processing;
   
   o if the processing is carried out within the scope of legal activity of an institution, association or any other non-profit entity, provided that such processing relates solely to the members of this entity, and that the data obtained is not disclosed to a third party without the prior consent of the individual;
   
   o if data processing is necessary to establish, obtain or protect claims prescribed by law;
   
   o when the individual personally published such data; and
o if data processing is necessary for the purpose of preventive medicine, medical diagnosis, health care or management of health institutions, on the condition that the data is processed by a health official based on the rules and regulations adopted by competent authorities.

B. the data collection of sensitive data is labelled as such; and

C. the controller has ensured sufficient technical protection of such data, in accordance with the Regulation on Technical Protection of Sensitive Data (the Regulation may be found at: http://azop.hr/page.aspx?PageID=79).

Personal data pertaining to misdemeanour and criminal records may be processed exclusively under the control of competent authorities.

f. Employee Personal Data

The collection and processing of employees’ personal data is regulated by both the Act and the Croatian Labour Act.

Under the Labour Act, employers are obliged to maintain a record of employees’ data containing “personal employees’ data” (generally interpreted as data necessary for the performance of the employer’s duties arising from the employment relationship, such as payment of salary), data on their working hours and data required by pension system rules.

Apart from this data, employers may generally collect other data related to or necessary for the purposes of the employment relationship, provided that the mandatory provisions of the Act are observed.

5. Consent

a. General

Under the Act, an individual’s consent means any freely given, informed and clear statement given by the individual towards approving the processing of his/her personal data for a specific purpose of which he/she has been notified.

In Croatia, consent is not mandatory for collection and/or processing of personal data – rather – it is only one of the grounds under which personal data may be legally collected and processed.

b. Sensitive Data

Consent for collection of sensitive data in Croatia is required only in the absence of other statutory grounds for the collection of such data. For more details on this question, please see Section 4(e).

c. Minors

The Act does not contain any special provisions regarding the minor’s consent.
Rather, it only stipulates that any minor’s personal data may be collected and processed only “in accordance with the Act and by implementing special security measures set in other statutes”. The DPA to date has not issued any guidance or opinion specifying these statutes. Presumably, a special provision would apply in specific cases regulated by relevant laws, such as for example, in case of misdemeanor or criminal procedures against minors.

However, the DPA has in several decisions noted that a minor’s consent actually should be interpreted as consent of their parents (or other legal guardians).

d. Employee Consent

Typically, an individual’s consent to data collection is required only in case if the collection cannot be justified under some other grounds provided in the Act.

In case of data collection from employees, an employee’s consent would not be required as long as (i) data collection is necessary for the performance of the employer’s statutory obligations (e.g., collecting data required under labour law legislation as explained under Section 4(f), or (ii) data collection is necessary for the purposes of the employee’s employment (e.g., taking the employee’s photo in order to upload it on the employer’s webpage), or (iii) if the employer has a legitimate interest for such collection (e.g., if certain data is necessary for the restructuring of its business).

Should the collection of personal data go beyond these limits, an employee’s consent would be required.

e. Online/Electronic Consent

The Act does not expressly prescribe the required form in which the individual would have to give his/her consent, although it requires for the consent to be explicit.

With reference to the Croatian rules on contractual obligations, it is a general practice that consent may be given in any suitable form as long as it is explicit, clear and, to the extent possible, gives a suitable impression that it is freely given.

6. Information Requirements

The Act prescribes elaborate information compliance requirements, similar to the ones set out in the Directive.

Prior to collecting any personal data, the data controller (or the data processor) must inform the individual whose personal data is being collected about:

- identity of the data controller;
- intended purpose of processing his/her data;
right to access the collected data;
right to correct the collected data;
recipients or categories of recipients of the collected data;
whether the data collection is voluntary or mandatory;
the possible consequences of withholding the data; and
(in case of mandatory collection of such data), the legal basis for personal data processing.

As an exception to the above, such information does not have to be provided to the individual if (i) data is merely given to be used or is collected from existing personal data files in order to be processed for statistical purposes or for the purposes of historic or scientific research, or (ii) informing the individual would require an excessive effort, or (iii) such processing of personal data has been explicitly allowed by law.

7. Processing Rules

According to the Act, the data controller is responsible to ensure that personal data:

- is collected only for the purpose explicitly provided for and subsequently processed only for that purpose or for a purpose related with that purpose;
- such purpose is known to the individual;
- is relevant for the accomplishment of the established purpose and is not collected in larger quantities than necessary for achieving such purpose;
- is accurate, complete and up-to-date; and
- is kept in a form which permits identification of the individual for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

Personal data collected and processed in accordance with these rules will be deemed valid in Croatia.

8. Rights of Individuals

Under the Act, individuals have the following rights towards data collectors:

- **Right to Access Personal Data.** Within 30 days from receipt of the individual’s request, data collectors must grant the individual access to his/her personal data and provide all relevant information related to the individual’s personal data that is being processed and deliver notices, excerpts, statements and all other relevant documents in its possession.
• **Right to Withdraw the Consent.** If the individual’s personal data is being processed based on his/her consent, the individual is entitled to withdraw his/her consent at any time.

• **Right to Modify/Erase.** At the individual’s request, the data collector must supplement, modify and/or erase any incorrect or otherwise incomplete individual’s personal data or if such data is not processed in accordance with the applicable laws. Related to the right to modify/erase, in case that the data collector independently establishes that the personal data in their databases is incorrect or otherwise incomplete or not being processed in accordance with the applicable laws, he/she is obliged to supplement, modify, and/or erase all such data and notify the individual on such amendments within a 30-day period.

In case an individual believes that any of his/her rights has been violated by illegal data collection or processing, he/she may report such breach to the DPA, which will decide on the alleged breach in an administrative proceeding. Should the DPA find that the individual’s right to privacy has been breached, it may order the data processor to cease the activities breaching the right to privacy. The DPA’s finding may be later used for a damages claim before the competent court.

9. **Notification/Registration Requirements**

Under the Act, data collectors must report every collection and processing of personal data to the DPA. The reporting is done by registration of a database with the Data Protection Register administered by the DPA ("Register"). This process consists of two steps.

1) **Prior to actual registration of a database or amendment of an existing registration** (by registering, for example, the fact that the data in the database is transferred out of Croatia or otherwise re-processed), data collectors are obliged to notify the DPA about the intention of such registration. The notification should be made prior to commencing the collection of personal data or actual processing.

   This obligation to notify the DPA does not apply if a special statute requests such data collection and/or processing in individual cases.

2) **Once the personal data is collected and a database is compiled, or when the processing has been performed,** the data collector is also obliged to register with the Register such database or the fact of processing of an existing database. These registrations should be made within 15 days from the creation of the new database or the performance of the processing action.
10. Data Protection Officers

The obligation to appoint data protection officers in Croatia is set out both in the Act and the Croatian Labour Act.

Under both statutes, employers hiring 20 or more employees are obliged to appoint a data protection officer who is in charge of monitoring the collection, processing, use and transfer of employees’ personal data. In particular, the data protection officer must:

- ensure that data processing is performed in accordance with applicable laws;
- inform all persons working on personal data protection about their legal obligation to protect personal data;
- ensure the exercise of the individual’s rights as provided in the Act; and
- cooperate with the DPA on implementing the supervision of personal data processing.

Data protection officers are appointed by a written decision of the employer which has to be delivered to the DPA within one month from the appointment. The DPA maintains the Register of Data Protection Officers.

11. International Data Transfers

As a rule, data controllers are free to execute international data transfers under the following conditions:

A. the country or organization to which personal data is being transferred provides an adequate level of data protection. The countries with an adequate level of protection of personal data include all EU Member States, three EEA countries (Norway, Liechtenstein and Island) and some other countries that can be found at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm;

B. the individuals have been informed of the transfer; and

C. the transfer has been registered with the Register in the relevant data controller’s database.

In case that the “adequate level of protection” requirement is not satisfied, the data collector must obtain an “opinion” from the DPA that the data transfer in that particular case can be legally executed. Under the Act, in case that a country where personal data is being transferred to does not provide an “adequate level of protection”, data transfer may be executed only under one of the following conditions:

- if the individual consents to the transfer;
• if the transfer is essential for protecting the life or the physical integrity of the individual;

• if the data controller provides sufficient guarantees regarding the protection of privacy and the fundamental rights and freedoms of individuals by using contractual provisions regulating the transfer for which the DPA has established that they comply with the regulations in force governing personal data protection;

• if the transfer of data is necessary for the execution of a contract between the data controller and the individual;

• if the data transfer is necessary for the conclusion or execution of a contract between the data controller and a third person, and which is in the interest of the individual;

• if the data transfer is necessary or determined by law for protecting public interest or to establish, obtain or protect the claims prescribed by law; or

• in case that data is being transferred from a database that is available to the public under law, data transfer may be executed in a degree (with respect to the documents) to which the applicable statutes allow for such transfer in each individual case.

In practice, even though the Act refers to the DPA’s input in case of international data transfers as an “opinion”, it should in fact be understood as a consent for such a transfer. The current practice of the DPA when it comes to exporting personal data abroad is very rigid and formal. Even a slightest lack in form may result in the DPA refusing to issue the necessary “opinion”.

12. Security Requirements

The data controller and recipient of personal data are obliged to ensure that appropriate and proportionate technical, staffing and organizational measures aimed at protecting personal data are in place.

These measures should protect personal data from (i) accidental loss or destruction, (ii) unauthorized access, (iii) unauthorized alterations, (iv) unauthorized dissemination, and (v) all other forms of abuse. Furthermore, the data controller and recipient of personal data must ensure that all persons entrusted with the processing of personal data sign a confidentiality statement.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Croatian laws allow for outsourcing of data processing to third parties (data processors). Under the Act, a data processor may only be a legal or natural person which is (i) registered for performing data processing activities, and (ii) which can secure a sufficient level of protection for the outsourced data.
Data processing can be outsourced to data processors only by a written agreement between the data controller and data processor. The data processing agreement must contain the clauses obliging the data processor to:

- process outsourced data exclusively in accordance with data controller’s orders;
- refrain from providing outsourced data to any third persons;
- process outsourced data only for the purpose set out in the data processing agreement; and
- ensure that the appropriate technical, organizational and staffing measures are in place for personal data protection.

In case of an occurrence of data breach, the outsourcing organization may be held liable together with the data processor.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, civil actions (including damages claims) and/or criminal liability.

With respect to administrative fines, under the Act they range between approximately USD 3,200 to USD 6,400 for entities and between USD 1,000 to USD 2,000 for the responsible individual within the entity. For misdemeanours set out by the Labour Act, the fines for entities can range up to USD 17,000, while the fines for the responsible individuals within the entity are the same as under the Act.

With respect to criminal liability, the Croatian Criminal Code prescribes imprisonment for up to one year for unauthorised collection, processing or use of personal data. If the criminal act concerns a child or is committed on sensitive data, the maximum sentence is up to three years. To the best of our knowledge, in practice, privacy offences are not enforced by way of criminal prosecution by the State Attorney (although the DPA has in the last few years reported several offences to the State Attorney’s Office).

15. Data Security Breach

Under the Act, there is no duty to notify the individuals in case of a data security breach. In case of a data security breach, data controllers could be liable for misdemeanour (for failing to secure adequate security measures) and incurred damages to individuals (if any).
16. Accountability

Apart from (a very) general provision that the data controller and recipient must ensure that proportionate technical, staffing and organisational measures aimed at protecting personal data are in place, the Act is silent on the issue of accountability. However, although not expressly provided for in the Act, the DPA has in several of its opinions stated the importance of implementing the “Privacy by Design” approach, under which data controllers are responsible to regularly update their security system to be fit for its purpose and the categories of data it contains.

For more details on the issue of data security, see Section 12.

17. Whistle-Blower Hotline

Whistle-blower hotlines may generally be established in Croatia.

Organizations wishing to implement a whistle-blower hotline are required to: (i) include in the internal by-laws or other document detailing the employer’s IT policy a provision(s) on the scope and purpose of the whistle-blower hotline, (ii) notify its employees of its existence and the data it may collect, and (iii) notify and register the hotline as a database with the Register (as explained in Section 9 above).

As the Act does not provide any guidance regarding the whistle-blower systems, particular importance should be paid to its design, to make sure that it is proportionate to its purpose and does not collect more personal data than is necessary.

18. E-Discovery

The Croatian legal system does not recognize nor use the institute of discovery, including e-discovery.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to: (i) include in the internal by-laws or other document detailing the employer’s IT policy a provision(s) on the scope and purpose of the anti-spam filtering, (ii) inform employees of the monitoring policies being implemented in the workplace, and (iii) if applicable, notify and register the anti-spam filter as a database with the Register (as explained in Section 9 above).

In any case, filtering should be executed as a generic surveillance of types of messages, and not as surveillance of the content of individual employees’ emails.
20. Cookies

Cookie compliance in Croatia is regulated by the Electronic Communications Act. However, the data protection “aspect” of the cookie compliance is that the “user’s consent” is interpreted in line with the Act.

The Electronic Communications Act requires webpage owners to make sure that users give their explicit informed consent to the use of cookies (“opt-in” approach). This would involve, for example, a pop-up window informing the user on the use of cookies together with ticking a check-box for consent to use them and clicking the “continue” tab.

21. Direct Marketing

The use of personal data in direct marketing will depend on whether such data is obtained directly from individuals or in some other manner.

The Act envisages only the situation where personal data is obtained directly from the individuals. In such cases, businesses that wish to use personal data in marketing services must inform the individual that they wish to use his/her personal data for marketing services and about his/her right to refuse such use. Even if the individual does not initially object to the use of his/her data for marketing purposes, he/she may withdraw his/her consent at any later point, in which case direct marketing must cease.

In case that businesses conduct their direct marketing activities using data not directly obtained from individuals (by, for example, random selection of phone numbers or by using data that was collected by a third party), they are not required to ask in advance whether they can perform marketing activities using the individual’s personal data. However, individuals still have the right to withdraw their (implied) consent for such marketing, in which case all marketing activities must cease.

Should businesses not comply with the individual’s request to cease marketing activities, they would be held liable for a misdemeanour in accordance with the Act.
Czech Republic

Jiri Cermak
Prague
Tel: +420 236 045 001
jiri.cermak@bakermckenzie.com

Milena Hoffmanova
Prague
Tel: +420 236 045 001
milena.hoffmanova@bakermckenzie.com
1. Recent Privacy Developments

**Opinion of the Office for Personal Data Protection on the redundant obtaining of consent to statute-based processing of personal data**

In August 2014, the Office for Personal Data Protection issued an opinion regarding the redundant obtaining of consent from the Data Subjects to processing of their Personal Data in cases where such processing is based on statutory legal grounds. The Office articulated that where the processing of Personal Data is imposed upon a Data Controller by a statute (e.g., processing of Personal Data pursuant to the Act on Selected Measures Against Legitimization of Proceeds of Crime and Financing of Terrorism), it is redundant to request consent of the Data Subject to such statute-based processing. The Data Controller is obliged to process Personal Data irrespective of whether the Data Subject consents thereto or not. Therefore, obtaining consent in such cases is misleading and confusing to the Data Subject, given that the Data Subject may believe revoking his/her consent would terminate the processing. The above redundancy in obtaining the consent amounts to a violation of the obligation of the Data Controller to duly inform the Data Subject about the nature of the data processing, as the Data Subject might incorrectly rely on the possibility of revoking the consent in instances where the data processing is statute-based.

2. Emerging Privacy Issues and Trends

There are no new developments in the Czech Republic.

3. Law Applicable


4. Key Privacy Concepts

**a. Personal Data**

The CDP applies to the processing of any information relating to natural persons (“Data Subjects”) who can be identified either directly or indirectly from that information, in particular by reference to a number, code or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity (“Personal Data”).

**b. Data Processing**

According to the CDP, processing of Personal Data means any operation or a set of operations, systematically executed by a Data Controller (see Section 4(c) below) in an automatic or other manner. Processing means, in particular, the collection of Personal Data, its storage on data carriers, retrieval, modification or alteration, searching, using, transferring, distributing, publishing, preserving, exchanging, sorting or combining, blocking or liquidating (i.e., deleting or destroying) Personal Data.
The CDP applies to any processing of Personal Data, whether executed automatically (e.g., electronically) or otherwise and thus both hard and soft/electronic copy of records of Personal Data are covered by the CDP and considered data carriers.

The CDP does not apply to Personal Data processed for purely personal purposes or the occasional collection of Personal Data which is not subsequently processed any further.

c. Processing by Data Controllers
Any person or entity (e.g., an employer) who specifies the purpose and the means of the processing of Personal Data, executes such processing and is responsible for it, is viewed as a Data Controller (“Data Controller”) for the purposes of the CDP.

d. Jurisdiction/Territoriality
The CDP applies to processing carried out by Data Controllers established in the Czech Republic as well as foreign-established Data Controllers that process Personal Data in the Czech Republic, except for the transfer of Personal Data through the territory of the European Union (including the Czech Republic).

e. Sensitive Personal Data
The CDP imposes additional requirements for the processing of Sensitive Personal Data - that is, data relating to nationality, racial or ethnic origin, political attitudes, membership of trade unions, religious and philosophical beliefs, criminal convictions, health conditions and sexual life, genetic data of the Data Subject, or biometric data, which enables the Data Controller to directly identify or authenticate the Data Subject.

Sensitive Personal Data may be processed only if the Data Subject has given explicit consent (in writing) to such processing. However, the CDP stipulates that the consent is generally not required if:

- the processing is necessary to protect the vital interests of the Data Subject, or to address an immediate danger threatening his property, and where the Data Subject is physically, mentally, or legally incapable of giving consent, or is missing, or because of any similar reason;
- the processing is necessary for providing health care, public health protection, health insurance, public administration in the area of healthcare, or examination of health conditions pursuant to a specific law;
- the processing is necessary to fulfill the obligations and rights of the Data Controller in the field of employment or labor law (arising under a specific law);
the processing (i) is carried out in the course of legitimate activities by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade union aim, (ii) is duly authorized, (iii) relates only to the members of such a body, and (iv) Personal Data is not disclosed without the consent of the Data Subject;

- the processing of Personal Data is required to provide health insurance, social security insurance, old age pension security, state social subsidy and other social care according to specific laws;
- the processing relates to Personal Data that is made public by the Data Subject;
- the processing is necessary for the establishment or exercise of legal claims;
- Personal Data is processed only for archiving purposes pursuant to a special law; or
- the processing is carried out according to special laws in the course of prevention, investigation, detection of criminal activity, prosecution of criminal offenses and searching for individuals.

f. Employee Personal Data

The CDP does not recognize a special category of employee Personal Data and, therefore, the general rules for processing set forth in the CDP apply. However, in the case of an employment relationship, if the scope of Personal Data collected does not exceed the scope of data required for concluding or performing an employment agreement under the Czech Labor Code, employee consent (as described in Section 5(a) below) and notification to the Office would not be required. However, the Labor Code does not specifically state what Personal Data is necessary for concluding or performing an employment relationship.

Sensitive Personal Data, by its definition, does not fall within the scope of employee Personal Data which can be collected and processed without the employee’s consent. Nevertheless, it is generally acknowledged by the Office, that any Personal Data that is collected for the purpose of an employment agreement and granting of additional employee benefits can be collected without the employee’s consent (e.g., data regarding name, address, date of birth, citizenship, phone numbers, education, salary, bonus, social security, bank account, etc.).

A fallback justification for processing both Personal Data and Sensitive Personal Data in the employment context is when the employee as the Data Subject provides consent.
According to the CDP, the fact that Sensitive Personal Data belongs to an employee is not relevant in respect of the rules for processing of such Personal Data. Accordingly, processing of Sensitive Personal Data in excess of the scope permitted under the Labor Code must be justified by the employee’s consent or another ground in Section 4(e).

5. Consent

a. General

Under the CDP, the general rule is that a Data Controller may process Personal Data as long as the consent of the Data Subject is obtained. However, CDP provides for a number of exceptions.

Consent must be voluntary, informed, explicit and unambiguous, and must be obtained prior to or at the time of collection of data. Consent only covers identified purposes, and hence, fresh consent is needed for purposes not previously identified and consented to. The Data Subject can revoke the consent at any time.

The CDP does not stipulate in what language consent must be given. The Office regularly communicates in the Czech language; however, in practice, the Office is flexible in this area and usually accepts documents in the English language as well. In addition, consent can be translated into the Czech language should the Office so require.

b. Sensitive Data

Subject to specific exceptions stipulated in the CDP, Sensitive Personal Data may be processed only if the Data Subject has given explicit consent (in writing) to such processing. Prior to giving consent to the processing of Sensitive Personal Data, the Data Subject must be informed of (i) the purpose(s) of processing for which the consent is given, (ii) the scope of the Personal Data being processed, (iii) the Data Controller to which the consent is given, and (iv) the period of time for which the consent is given. The Data Controller must be able to prove the existence of the consent during the entire period of the processing of Personal Data and the Data Subject can revoke the consent at any time.

c. Minors

According to the Czech Civil Code, a person becomes fully competent to acquire and assume rights and obligations through legal acts upon reaching the age of 18 years. However, the Civil Code also stipulates that minors (i.e., persons below 18 years of age) can execute such legal acts in law which correspond to the level of their mental and moral maturity. In addition, the Civil Code regulates certain specific rights of minors who have reached the age of 15 years (e.g., right to express last will).
In light of this, it has been generally acknowledged by the Office, that minors between 15 and 18 years of age can execute legal acts in relation to their Personal Data (i.e., can provide consent to Data Controller). The statutory representatives (e.g., parents) of a minor represent and act on behalf of minors that are below 15 years of age.

**d. Employee Consent**

There are no special rules or limitations stipulated in the CDP in relation to consent granted by an employee to the employer. Therefore, the general consent rules apply to employee Personal Data.

**e. Online/Electronic Consent**

Consent can also be given electronically as long as the Data Controller:

- assures that each consent can be unequivocally assigned to a particular identified Data Subject, and the consent includes all required information. An electronic signature that meets the requirements set forth in the Czech Act on Electronic Signatures (implementing EU Directive 1999/93/EC) provides the highest standard of legal certainty with respect to identification of the acting person. It is therefore advisable to comply with these requirements wherever possible.

**6. Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity, the types of Personal Data being collected, the purposes for collecting Personal Data, third parties to which the organization will disclose the Personal Data, the consequences of not providing consent, the rights of the Data Subject, where the Personal Data is to be transferred, how to make an inquiry or file a complaint, how to access and/or correct the Data Subject’s Personal Data, and the duration of the proposed processing.

**7. Processing Rules**

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

**8. Rights of Individuals**

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.
9. Registration/Notification Requirements

Generally, processing of Personal Data requires registration with the Office. Registration is not required if (i) only publicly available Personal Data is being processed, (ii) the processing is carried out on the basis of a special law or is necessary to fulfill the legal obligations and rights of the data controller, or (iii) the processing is carried out in the course of legitimate activities by a foundation, association or any other non-profit seeking body with a political, philosophical, religious or trade union aim, and the processing is duly authorized and relates only to the members of such a body.

Given the foregoing, before commencement of processing of Personal Data, the Data Controller needs to notify the Office. The notification is carried out by filling in an online notification form available on the website of the Office.

10. Data Protection Officers

In the Czech Republic, there is no requirement for organizations to appoint a data protection officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

According to the CDP, Personal Data can be transferred:

- to EEA member states without any limitation; and
- to third countries (i.e., non-EEA countries) if (i) such transfers are permitted under a ratified international treaty binding on the Czech Republic or (ii) Personal Data is transferred on the basis of the decision of an EU authority.

If the abovementioned conditions are not met, Personal Data can only be transferred to recipients outside the Czech Republic if:

- the Data Subject has given consent to or instructions for the transfer;
- the recipient’s country provides sufficient special safeguards for protection of Personal Data which are specified in an agreement between the Data Controller and the recipient of the transferred Personal Data, provided that such an agreement: (i) ensures application of the special safeguards or (ii) includes the standardized contractual clauses published in the Office’s Gazette. In addition to the EEA countries, the Office considers, *inter alia*, Switzerland, Norway, Argentina, Faeroe Islands, Guernsey, Jersey, Iceland, the Isle of Man, Canada, Andorra, Liechtenstein and Israel as providing sufficient special safeguards for cross-border data transfer. Although the Office does not consider the US to be a “safe” country in this respect, Data Controllers can benefit from the Safe Harbor Agreement when transferring Personal Data to recipients located in the US;
the transfer is made from a public register or a register accessible to everyone who proves a legal interest;

- the transfer is necessary for the establishment or exercise of an important public interest arising under a special Act or an international treaty binding on the Czech Republic;

- the transfer is necessary for the performance of a contract to which the Data Subject is party, or if the processing is essential for the Data Subject to enter into negotiations for the formation of a contractual relationship or for the amendment of an existing contract;

- the transfer is necessary for the conclusion or performance of a contract entered into between the Data Controller and third parties in the interests of, or at the request of, the Data Controller; or

- the transfer is necessary for the protection of the rights or vital interests of the Data Subject, especially for the protection of the Data Subject’s life or provision of healthcare.

Subject to the exemptions provided by (i) international treaties binding on the Czech Republic (e.g., the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (“Convention 108”), to which the Czech Republic is a signatory), or (ii) decisions of the competent bodies of the European Union (e.g., decision No. 2000/520/EC of the European Commission on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce), the Data Controller must apply for Office approval in relation to every transfer of Personal Data to a third country (i.e., non-EEA country).

Since the Czech Republic is a signatory country to Convention 108, the provisions of Convention 108 supersede the provisions in the CDP regarding the transfer of Personal Data to other countries.

According to Article 12 of Convention 108, a contracting state must not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization cross border flows of Personal Data going to the territory of another contracting state.

Article 12 applies to transfers across national borders, by whatever medium, of Personal Data undergoing automatic processing or collected with a view to being automatically processed.

At the time of writing, the following countries are contracting states to Convention 108: all EU countries, Albania, Andorra, Azerbaijan, Bosnia and Herzegovina, Croatia, Georgia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Romania, Russia, Serbia, Switzerland, the former Yugoslav Republic of Macedonia, Turkey, and Ukraine.
12. Security Requirements
Organizations are required to take steps to: ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
There are no specific rules for outsourcing in the Czech Republic. As long as the outsourcing entity complies with its duties as Data Processor and the Data Controller complies with its duties, the outsourcing may be considered valid. Special rules may however apply in certain sectors (such as the banking sector).

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
Generally, if there is a data security breach, the breach does not have to be reported under the CDP. However, given that a duty to prevent damage generally applies, any security breach that may cause damage to Data Subjects must be duly reported to them in order to allow them to adopt the appropriate course of action (e.g., change of the password, etc.). Such notice should be delivered to the Data Subjects as soon as possible in order to ensure that they will be able to prevent potential damage.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, and civil actions and/or class actions.

16. Accountability
Subject to regulatory guidance, organizations may be required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data, furnish the results of the privacy impact assessments to privacy regulators upon request, and furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.
17. Whistle-blower hotline

Whistle-blowing is not specifically regulated in CDP. Therefore, any processing of Personal Data carried out in connection with operation of a whistle-blowing hotline in the Czech Republic will be subject to general rules and obligations regarding the processing of Personal Data.

The CDP requires all persons intending to process Personal Data in relation to Data Subjects in the Czech Republic to register with the Office. Registration is not required, inter alia, if the processing is carried out on the basis of a special law or is necessary to fulfil the legal obligations and rights of the Data Controller arising under a special law (e.g., labor law, criminal law, etc.). Given the foregoing, in case of the processing of Personal Data due to a whistle-blowing hotline, an argument can be made that such processing is excluded from the general registration obligation according to the CDP on the grounds that the Data Controller fulfils the legal obligations and rights arising under law (e.g. prevention of occurrence of damage or breach of applicable laws).

However, given the fact that processing of Personal Data in connection with the whistle-blowing hotline is often carried out on the basis of requirements of a foreign law or statute (e.g., the US Sarbanes Oxley Act) rather than to fulfil the legal obligations arising under Czech law and such processing often exceeds the Personal Data processing that falls within the exception as stipulated above, it is generally recommended to register the respective Personal Data processing connected with the operation of the whistle-blowing hotline with the Office.

18. E-discovery

In general, the monitoring and recording of employees may take place only if the employees are informed that such monitoring is conducted and information such as e-mails will be stored, including the detailed list of the devices that are monitored. This is important since all employees should receive clear information about those areas where they can expect privacy and those that are under continuous or irregular surveillance by the employer.

Please note that strict privacy protection principles apply in the Czech Republic in relation to the employer’s monitoring of the employee’s activities and communication carried out during the time spent at work (including the monitoring of e-mails). According to these rules, without a serious cause consistent with and within the employer’s activities as an employer, the employer may not encroach upon employees’ privacy in the workplace and employer’s common premises by open or concealed surveillance (monitoring) of employees, interception (including recording) of telephone calls, or checking electronic mail or postal consignments addressed to a certain employee. Monitoring of the content of incoming correspondence addressed
19. Anti-Spam Filtering

Whether there are any regulatory concerns pertaining to the deployment of spam filtering technology is determined by considering the nature of the software that is implemented (i.e., whether the spam-filtering solution is automatic and applicable in the same manner for all of the employees or whether it allows certain IT officers of the company to monitor the content of the spam).

20. Cookies

There has been a transition in the regulatory regime from opt-out to opt-in requirements when it comes to deployment of cookies. The recent EU Directive 2009/136/EC calls for express prior consent, i.e., opt-in; nevertheless, the methods for giving such a consent remain rather broad. Particularly, within the Czech jurisdiction, according to the opinion of the Office, it is acceptable not only to provide express consent for the use of cookies by accepting the terms when opening a website, but also through setting the web browser to accept the cookies by default.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.
Denmark

Lisa Bo Larsen
Copenhagen
Tel: +45 38 77 45 68
lbl@kromannreumert.com

Daiga Grunte-Sonne
Copenhagen
Tel: +45 38 77 41 18
DSO@kromannreumert.com
1. Recent Privacy Developments

The key legislation regulating data privacy in Denmark is the Danish Act on Processing of Personal Data, Act no. 429 of 31 May 2000 with subsequent amendments (the Data Protection Act), which is based on EC Directive No. 95/46/EC of 24 October 1995 (the Data Protection Directive).

Within the last year (2014), no new legislative acts or amendments of significance to the Data Protection Act have been adopted. However, there have been amendments to the Danish Financial Business Act, which have resulted in a new set of financial whistle-blower rules that came into force on 1 September 2014. These rules require all financial institutions to implement a mandatory whistle-blower scheme that must offer:

- a special, autonomous and independent report channel (meaning independent of the daily management of the entity),
- access to report any violation of the applicable financial rules, regardless of the significance of the suspected violation,
- access to file a report anonymously,
- access to file a report for all Danish employees (no requirement about access to file reports for employees of other group entities or third parties), and
- access for the employees to file a report on the entity as such, on other employees and/or on board members.

In this respect, the interpretation of “financial institutions” is fairly broad and includes mortgage-credit institutions, investment trusts, financial services advisers, company pension funds, banks, financial services companies and the securities services.

Prior to the implementation of such scheme, the financial institution in question must submit an application to the Danish Data Protection Agency (the “DPA”), which is the local data protection supervisory authority, and await its approval. In addition, the institution must submit an application for processing of personal data in the HR department, unless such approval has already been granted by the DPA. The fee for approval of each application is DKK 2,000 (approximately EUR 270).

The scheme may be outsourced to a third party, either a supplier of whistle-blower hotline solutions or, for example, an intra-group entity, but the responsibility for ensuring compliance with the requirements under Danish law remains with the financial institution in question.

Further, Denmark is at the moment anticipating the coming EC General Data Protection Regulation (the “Data Protection Regulation”), which will replace the current and somewhat outdated Data Protection Directive from 1995 and
thus the Data Protection Act. Besides a greater harmonization in the area, the Data Protection Regulation will take globalization and technological developments into account as well as implement larger fines for non-compliance with the Data Protection Regulation (up to 100 million EUR or as much as 5% of a company’s yearly turnover). Such fines are substantially higher than any fine issued in Denmark (the highest fine was issued in 2003 and amounted to DKK 25,000, which corresponds to approximately EUR 3,360), which undoubtedly will bring more awareness amongst companies in relation to data protection issues. The Data Protection Regulation is currently awaiting the Council’s first reading and is expected to come into force in 2016.

2. Emerging Privacy Issues and Trends

The DPA has published four new guidelines focusing mainly on IT security in relation to the processing of personal data. The following areas have been highlighted:

- **Security of login to databases** containing personal data - according to the DPA’s guidelines, the security of such databases can be considerably increased by adding two layers of passwords. However, the two-layer passwords should not be the only measure in this respect, since new technologies can quickly outdate security measures that were very recently deemed appropriate and sufficient. For example, most banks in Denmark require two sets of passwords when a customer accesses his account from a computer, while access from a mobile phone only requires one password layer, which can potentially undermine the otherwise enhanced security on computers.

- **Transfer of sensitive personal data** - the DPA recommends that the data controller use an end-to-end encryption where such data is transferred electronically. Use of a sufficiently complex encryption key is recommended, and the DPA suggests the use of password protection for the encryption key, which under these circumstances should have at least the same complexity as the encryption key itself.

- **Erasure of personal data** - under the Data Protection Act, there is an obligation to erase personal data when there is no longer a legal reason for retaining the data. Such erasure must be effective and permanent, e.g., the data must be erased in a manner that excludes the possibility to restore the data through the use of reasonable means. Thus, erasure of data is not sufficient if the data is still retained but the user’s rights to access the data are limited or removed, where only the shortcuts to the data are removed or where the data is erased over time as it is being overridden by new data.

- **Transfer of personal data over the Internet** - the data controller must ensure that the transfer meets the requirements of confidentiality, integrity and authenticity. Confidentiality can be ensured by eliminating potential
risks of unauthorized persons accessing the data. Integrity can be ensured by eliminating potential risks of the data being altered during the transfer, and authenticity can be ensured by verifying that the sender and the receiver of the data are who they claim they are. In this respect, the DPA recommends use of encryption and digital signatures in order to fulfil the requirements.

Additionally, the DPA has issued a number of statements in relation to security breaches. The DPA has since 2003 until today seen an increase in cases concerning security breaches from around 20 cases per year to more than 80 cases on a yearly basis. This development is closely related to the increased digitization of key functions in society and has had an effect on both the private and the public sector. The security breaches experienced often appear to be external hacker attacks, taking advantage of weak points in data centrals in order to gain access to personal information about other individuals, specially targeting individuals with a public profile.

3. Law Applicable

As mentioned above, the primary legal source regarding data privacy and protection is the Data Protection Act, which entered into force in 2000. There have been many amendments to the Data Protection Act through the years, most recently in 2013. Additionally, as Denmark is part of the European Union and thus the Data Protection Act implements the Data Protection Directive, the decisions from the courts of Denmark as well as the European Court of Justice have relevance when interpreting the Data Protection Act.

Interpretation of the Data Protection Act and the current practice is also partly based on the earlier practice in accordance with the Act no. 293 of 8 June 1978 on Private Registers, which was effective prior to the adoption of the Data Protection Directive.


Collection and processing of data is to some extent also regulated by other legislation, for example, there are specific rules in the Financial Business Act and the Payment Services and Electronic Money Act as regards the financial sector. These separate set of rules are stricter than the Data Protection Act, thus, the Data Protection Act provides the minimum regulation and applies where other legislation does not provide a higher level of protection for the data subject.

The responses below relate specifically to the Data Protection Act but references to other legislation will be provided where relevant.
4. Key Privacy Concepts

a. Personal Data

Personal data is defined in the Data Protection Act as “any information relating to an identified or identifiable natural person (‘data subject’)”.

Hence, personal data must be considered as a broad concept, e.g., any information that in any way can be connected to a specific physical person, with the help of reasonable means, will constitute “personal data”, regardless of whether the data will be perceived as objective (facts) or subjective (opinions). This also includes encrypted information as long as the encryption key exists.

Information related to legal entities is not regarded as personal data. However, this does not apply to data related to one-man businesses.

Further, anonymous data is not regarded as personal data, which is based on the assumption that the anonymisation process is carried through effectively. The assessment in this respect is rather strict, for example, encrypted data will not be regarded as anonymous as long as the data controller or another party can make the data “readable” again and connect the data to a particular individual. Theoretically, only “one-way” encryption, e.g., when the encryption key is destroyed, will meet these requirements. However, the means of the anonymisation must be subject to a concrete assessment, as in practice it is impossible to prevent every attempt of decryption.

b. Data Processing

The Data Protection Act defines data processing as “any operation or set of operations which is performed upon personal data, whether or not by automatic means”.

Thus, all actions, including but not limited to collection, selection, transfer, searching and deletion are considered as data processing.

c. Processing by Data Controllers

The Data Protection Act applies to entities that are data controllers, e.g., any “natural or legal person, public authority, agency or any other body which alone or jointly with other determines the purposes and means of the processing of personal data”.

The entity processing data on behalf of the data controller is regarded as data processor. The data processor may only process data in accordance with the data controller’s instructions and such data processing must be governed by a written contract between the parties. The contract must stipulate that the data processor may only act on instructions from the data controller and that there must be implemented appropriate technical and organizational measures to protect data against accidental or unlawful destruction, loss or alteration,
unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the Data Protection Act.

d. Jurisdiction/Territoriality
The Data Protection Act applies to any data controller established in Denmark, when the activities relating to the processing of data take place within the EU/EEA.

Further, the Data Protection Act applies to any data processing carried out on behalf of Danish diplomatic representations.

The Data Protection Act will also apply if the data controller is situated outside the EU/EEA and the processing of data is carried out with the use of equipment situated in Denmark, unless such equipment is used only for the purpose of transmitting data through the territory of the EU/EEA. The Data Protection Act will moreover apply to the collection of data in Denmark for the purpose of processing outside the EU/EEA.

e. Sensitive Personal Data
Pursuant to the Data Protection Act, sensitive data is regarded as information revealing/concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life.

As a starting point, such data may only be processed with the data subject’s explicit consent.

Further, sensitive personal data may be processed if:

- processing is necessary to protect the vital interests of the data subject or of another person where the person in question is incapable of giving his consent, or
- processing relates to data which have been made public by the data subject, or
- processing is necessary for the establishment, exercise or defence of legal claims.

There are also a number of exceptions specifically related to the different categories of sensitive data, for example, information on trade union membership may take place when necessary for compliance with the labor law obligations, or different areas of practice, such as the area of criminal law or health care services.

Moreover, processing of data related to criminal offences, serious social problems or other purely private matters (such as divorce or death in the family) must be very limited, as these types of data are regarded as semi-sensitive under Danish law.
Processing of such data on behalf of a public administration may only take place, if it is necessary for the performance of the tasks of the administration and disclosure of the data to third parties must be very limited and may mainly be based on the data subject’s explicit consent.

Private persons and entities may only process such data with the data subject’s explicit consent or if the processing is necessary for pursuing legitimate interests which clearly override the interests of the data subject. The same applies for disclosure of the data to third parties.

f. Employee Personal Data

Collection and processing of employee personal data is regulated by the Data Protection Act. Thus, the basic principles of data processing will apply (please see Section 7) and the employer must comply with principles of processing of sensitive data (please see Section 4(e), above), when relevant.

The DPA must be notified of the employer’s processing of sensitive employee data prior to such processing actually taking place. The application for such processing can be submitted electronically and must be approved by the DPA. The approval triggers an administrative fee of DKK 2,000 (approximately EUR 270).

Further, the DPA has issued guidelines regarding control of the employees’ use of the Internet and e-mail. Such monitoring may only take place if:

- the employer has a legitimate interest in retaining copies of e-mails and logs of Internet use,
- the employee has been made aware of the fact that the employer keeps copies of e-mails and logs of Internet use,
- the employee is informed that the employer may review such copies and log-files, when suspicion of misuse arises, and finally,
- the e-mails that are marked “private” or otherwise have clearly private content must be excluded from the review.

5. Consent

a. General

Pursuant to the Data Protection Act, the data subject’s consent must be freely given, specific and informed.

The data subject must have been provided with adequate information regarding the processing of the data in order for the consent to be “informed”. Further, the consent must constitute a positive action by the data subject, meaning that a consent based on the silence or passivity of the data subject will not be regarded as sufficient.
Processing of data may always be based on the data subject’s consent. However, the data subject has a right to withdraw his consent at any given time, hence, the practical reality is that the data mostly is processed in accordance with the general processing rules where processing under certain circumstances is be permitted without the data subject’s consent (please see Section 7 for further description).

b. Sensitive Data
The requirements for a legally valid consent regarding sensitive data are the same as mentioned above under Section 5(a).

c. Minors
Minors, who under Danish law are individuals under 18 years of age, are not able to give a binding expression of will and are therefore not able to give a valid consent. In order to obtain a valid consent from a minor, the consent must be obtained from a parent or a legal guardian.

In relation to processing of data on behalf of a public administration, a minor’s expression of will shall be legally binding and effective in relation to particular actions or rights granted by the substantial law, for example, submission of certain applications or making certain decisions on his/her own behalf.

d. Employee Consent
The requirements for a legally valid employee consent are the same as mentioned above under Section 5(a).

e. Online/Electronic Consent
Online/electronic consent is permissible and will be equally binding as consent given in written or oral form, as long as the requirements mentioned under Section 5(a) are fulfilled. The burden of proof in this respect lies with the data controller.

6. Information/Notice Requirements
Where the personal data have been collected from the data subject, the data controller must provide the data subject with the following information:

1. the identity of the controller and of his representative;
2. the purposes of the processing of the data;
3. any further information which is necessary, taking into account the specific circumstances of the collection of the data in order to enable the data subject to safeguard his interests. Such information may include:
   (a) the categories of recipients (but not the particular recipients);
   (b) whether the response to the questions is voluntary, including possible consequences of failure to reply;
Where the data have *not* been obtained *directly* from the data subject, the controller must provide the data subject with the following information:

1. the identity of the controller and of his representative;
2. the purposes of the processing of the data;
3. any further necessary information, such as
   (a) the categories of data;
   (b) the categories of recipients;
   (c) the rules on the right of access to and the right to rectify the data.

This information must be provided no later than the time when the data are disclosed, which in practice means within 10 days.

### 7. Processing Rules

There are a number of basic principles in relation to processing of data. Generally, the data controller must always comply with good practice for the processing of data, which means inter alia that the processing must be fair and reasonable. Further, following principles apply:

1. The data must be collected solely for specified, explicit and legitimate purposes and further processing must not be incompatible with these purposes.
2. The processed data must be adequate, relevant and not excessive in relation to these purposes.
3. The data must be updated when relevant and there must be carried out necessary checks to ensure that no inaccurate or misleading data are processed or retained. Data, which turn out to be inaccurate or misleading must be erased or rectified without delay.
4. The collected data may not be retained for a longer period than it is necessary for the purposes for which the data are processed.

As a general rule, personal data may only be processed if there is obtained an explicit consent from the data subject. The data may, however, also be processed without the data subject’s consent provided that processing is necessary:

- for the performance of a contract where the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

  (a) for data controller’s compliance with a legal obligation; or
(b) in order to protect the vital interests of the data subject; or

(c) for the performance of a task carried out in the public interest; or

(d) for the performance of a task carried out in the exercise of official authority vested in the controller; or

(e) for the purposes of the legitimate interests pursued by the data controller where these interests are not overridden by the interests of the data subject (the rule of balancing of interests).

Sections (e) and (f) apply equally to disclosure of data to third parties.

8. Rights of Individuals

The data subject has a right to access the data related to him. If the data subject submits a request to that effect, the data controller must inform him whether or not data relating to him are being processed. If the data controller processes such data, the following information must be communicated to the data subject:

1. the data that are being processed;
2. the purposes of the processing;
3. the categories of recipients of the data; and
4. any available information about the source of such data.

Such requests must be replied to without delay, e.g., soonest possible. If it is not possible to provide a reply within 4 weeks, the data controller must inform the data subject of the grounds for this and when the reply can be expected.

The data subject has a right to receive the information mentioned above twice a year. Thus, the data subject is not entitled to a new communication in this regard until 6 months after the last communication, unless he can establish that he has a specific interest to that effect.

The data subject may at any time object to the processing of data relating to him. Where this objection is justified, the processing may no longer involve the particular data. An objection will be considered justified if the processing is illegal, or the particular circumstances of the case justify the objection. This can for example be the case, where an employee wishes to have his contact information removed from the employer’s website due to harassment from a former spouse.

In addition, the data controller must at the request of the data subject rectify, erase or block data, which turn out to be inaccurate or misleading or in any other way processed in violation of law or regulations. The data controller must also notify the third party to whom the data have been disclosed of any such rectification, erasure or blocking. However, this will not apply if such notification proves impossible or involves a disproportionate effort.
9. Registration/Notification Requirements

In respect of processing operations carried out on behalf of a private data controller and the notification obligation of such processing, the theoretical main rule under the Data Protection Act is that the processing must be notified with the DPA before its commencement. However, the practical reality is that notification is only necessary when processing involves sensitive data, as many processing operations of data are, in fact, exempt from the notification obligation. The notification obligation is particularly relevant in relation to processing of employee data - please see Section 4(f).

The exemption to the notification obligation can be found in both the Data Protection Act and in the Executive Orders No. 534 of 15 June 2000 and No. 410 of 9 May 2012 regarding exemptions to the notification obligation of certain processing operations carried out on behalf of a private controller.

If a data controller is obliged to notify a processing of data, the data controller must notify the DPA prior to the commencement of the processing and such notification must include the following information:

- the name and address of the data controllers and of their representatives, if any, and of the data processors, if any;
- the category of processing and its purpose;
- a general description of the processing;
- a description of the categories of data subjects and of the categories of data relating to them;
- the recipients or categories of recipients to whom the data may be disclosed;
- intended transfers of data to third countries and statutory authority for such transfers (e.g., EU standard model clauses, Safe Harbor certifications, binding corporate rules etc.);
- a general description of the measures taken to ensure security of processing;
- the date of the commencement of the processing; and
- the date of erasure of the data.

Notification must be made for every separate processing, or alternatively for multiple processing for which one overall purpose applies. This could be the case with different data processing connected to one specific assignment.

The notification form can be downloaded from the website of the DPA (www.datatilsynet.dk) and can be filed electronically, by e-mail or by ordinary mail. The notification must be filed in Danish.
With respect to processing carried out on behalf of a public administration body, the theoretical main rule under the Data Protection Act is that the processing needs to be notified prior to its commencement. However, the practical reality is that notification is only necessary in certain situations, when processing so-called data of a confidential nature. Under Danish law, data can be ‘of a confidential nature’ either when defined confidential by law or when its secrecy is necessary to safeguard essential public or private interests. Consequently, ‘data of confidential nature’ covers a wider scope of data than sensitive data.

The exemptions to the notification obligation can be found both in the Data Protection Act and in Executive Order No. 529 of 15 June 2000 on exception from the obligation to notify certain processing carried out on behalf of the public administration.

10. Data Protection Officers

In Denmark, it is not a requirement to appoint or designate a data protection officer or other individual who will be accountable for the data protection practices of the legal entity or the public body. The current legal position in this respect is, however, expected to change when the Data Protection Regulation is adopted.

11. International Data Transfers

Any transfer of personal data to a third country, e.g., outside EU/EEA, may only take place if the third country in question ensures an adequate level of protection.

The adequacy of the level of protection afforded by a third country must be assessed in light of all the circumstances in relation to the data transfer operation, in particular (i) the nature of the data, (ii) the purpose and duration of the processing operation, (iii) the country of origin and the country of final destination, (iv) the rules of law in force in the third country in question and (v) the professional rules and security measures which are complied with in that country.

In addition, transfer of data to a third country may take place if:

1. the data subject has given his explicit consent; or
2. the transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken in response to the data subject’s request; or
3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
4. the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
5. the transfer is necessary in order to protect the vital interests of the data subject; or
6. the transfer is made from a register which according to law or regulations is open to consultation either by the public in general or by any person who can demonstrate legitimate interests, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case; or
7. the transfer is necessary for the prevention, investigation and prosecution of criminal offences and the execution of sentences or the protection of persons charged, witnesses or other persons in criminal proceedings; or
8. the transfer is necessary to safeguard public security, the defence of the realm, or national security.

Outside the scope of the transfers referred to in nos. 1 - 8, the DPA may authorize a transfer of personal data to a third country which does not have an adequate level of protection, where the controller adduces adequate safeguards with respect to the protection of the rights of the data subject. Specific conditions may be laid down for the transfer. The DPA must inform the European Commission and the other Member States of the authorizations granted pursuant to this provision.

The transfer of personal data to third countries may be carried out without authorization from the DPA on the basis of contracts in accordance with the standard contractual clauses approved by the European Commission (EU standard model contracts), provided that the wording of these contractual clauses is not amended.

Further, transfer of data to the entities established in the USA may take place without authorization if the entity in question is Safe Harbor certified. However, this does not apply for transfers of sensitive data where such authorization still is necessary.

Groups of companies where the entities are established in many different jurisdictions may with advantage choose to prepare a set of binding corporate rules (BCR) for data transfers within the group. The binding corporate rules must be approved by a supervisory authority in one of the EU Member States (including Denmark) which then will coordinate the approval process with the other involved local data protection supervisory authorities. When this approval is granted, no separate local approval of the BCR in Denmark is necessary. However, a separate approval for the transfer based on the BCR must be obtained from the DPA. Also, the BCR will be basis for transfer of data only (e.g., the receiving entity is a data processor) and not for disclosure of data where other grounds will be necessary.
12. Security Requirements

The data controller must implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, loss or alteration, unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the Data Protection Act. The same applies to data processors.

In practice, this means that the entities must ensure limited and only authorized access to the data, effective procedures in this respect, use of passwords, firewall or other antivirus programs, encryption, etc. Where personal data is transferred through the internet, it must be done through a secure connection.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

The data controller may outsource the processing of data to a third party, under the assumption that the data processor acts in accordance with the instruction from the data controller, and that any action taken by the data processor will be considered as made by the data controller. The data controller must ensure the data processor’s compliance with the Data Protection Act.

14. Enforcement and Sanctions

If the data controller breaches his obligations under the Data Protection Act, or does not act in accordance with a decision made by the DPA, the data controller may be liable for a fine or punished with imprisonment of up to four months (individuals only). However, imprisonment as a sanction is very unlikely.

In Denmark, the level of fines is rather low - between DKK 3,000 and DKK 10,000 (EUR 403 - EUR 1,343). As mentioned in section 1, the highest fine until now amounted to DKK 25,000 (EUR 3,360).

Selling access to a non-public protected information system, which contains personal or sensitive data, can be punished with imprisonment of up to six years in severe cases. This applies to individuals only.

In addition, any breach of the obligations under the Data Protection Act may constitute grounds for liability to the extent the data subject suffers damages, should these be monetary or integrity related.

15. Data Security Breach

Currently, there is no requirement to notify the data subjects or the DPA when a data security breach occurs.
However, the DPA requires that in situations where personal data have been leaked to the public against the rules of the Data Protection Act, the data controller must, depending on the situation and the particular circumstances, as soon as possible attempt to:

- delete data from the Internet, search engines etc.,
- have the data returned from wrong receivers,
- notify the relevant data subjects and,
- implement long-term measures to ensure that such incidents will not take place in the future.

16. Accountability

The data controller does not have any legal obligation to prepare documents like privacy policies, IT policies etc. or to generally document any data protection impact assessments. However, the reality is that such documents often provide the necessary or appropriate solutions for fulfilling the obligations under the Data Protection Act, such as providing the necessary information to the data subjects or ensuring the data processor’s compliance with the provisions of the Data Protection Act.

17. Whistle-Blower Hotline

Whistle-blower hotlines are permissible in Denmark subject to a prior permission from the DPA. The DPA generally takes the view that such hotlines should be a voluntary alternative to the entity’s usual lines of communication. Thus, it should not be mandatory for the employees to raise their concerns through the whistle-blower hotline.

Only reporting of serious offenses are permissible via the hotline, e.g., offences, which amount to serious misconduct or suspected serious misconduct which may affect the entity as a whole or which may have a decisive impact on the life and health of individuals. Such matters are undoubtedly serious economic crime, including bribery, fraud, forgery and similar offences as well as irregularities in the areas of accounting and auditing, internal controls or financial reporting, anti-competition and insider trading. Other examples of incidents that may be reported include cases of environmental pollution, serious violations of occupational safety rules and serious offences against an employee, for instance violence or sexual offences.

Further, the DPA has accepted that incidents falling within the US Sarbanes-Oxley Act may be reported, e.g., accounting, internal control and audit irregularities, and suspected corruption and banking crimes.
However, less serious misconduct should not be capable of being reported, including for example cases of mental bullying, collegial difficulties, incompetence, absence, and breach of dress codes, smoking and alcohol policies and workplace rules on the use of e-mails/Internet, etc. In cases like this, the usual lines of communication should be used instead.

Finally, the Data Protection Act requires the whistle-blower hotline to be designed only with a view to reporting persons who are related to the entity such as employees, members of the board of directors, auditors, lawyers, suppliers etc.

The entity has the obligation to inform its employees of the existence and the functions of the whistle-blower hotline and must also have specific procedural rules on how to handle the given information, both concerning the person reporting the incident and the data subject.

Anonymous reporting is permissible, if necessary; however, employees and board members should not be encouraged to report anonymously.

Prior to implementation of the whistle-blower hotline, the entity must submit an application to the DPA), which will trigger an administrative fee of DKK 2,000 (approximately EUR 270) upon approval. The entity must also submit an application for processing of personal data in the HR department, unless such approval has already been granted by the DPA (the fee of DKK 2,000 (approximately EUR 270) applies here as well).

As regards the whistle-blower hotlines in the financial sector, special rules apply - please see Section 1.

18. E-Discovery

In Denmark, e-discovery is not used in civil litigation and will only be relevant in criminal cases.

19. Anti-Spam Filtering

As anti-spam filter solutions involve monitoring, the employees must be informed of implementation of such measure. Please see Section 4(f).

20. Cookies

The use of cookies is regulated by Executive Order no. 1148 of 9 December 2011 on Information and Consent Required in Case of Storing and Accessing Information in End-User Terminal Equipment (the Cookie Order), which is based on EC Directive no. 2002/58/EF of 12 July 2002. The Cookie Order requires collection of explicit and informed consent from the user prior to placing cookies on the user’s computer or other electronic device.
The user must be provided with comprehensive information about the storing of, or access to, the information collected via cookies. The information will be regarded as sufficiently comprehensive if:

a) it appears in a clear, precise and easily understood language or similar picture writing;

b) it contains details of the purpose of the storing of or access to information in the end-user's terminal equipment;

c) it contains details that identify any natural or legal person arranging the storing of, or access to, the information (e.g., also third parties);

d) it contains accessible means by which the end-user can refuse consent or withdraw an already given consent;

e) it contains clear, precise and easily understood guidance on how the end-user should make use thereof, and

f) it is made immediately available to the end-user by being communicated fully and clearly to the end-user.

The Danish Business Authority, which is the supervisory authority as regards the use of cookies, has issued guidelines on the Cookie Order.

21. Direct Marketing

Use of personal data for the purposes of the data controller’s own direct marketing must comply with the general processing rules (please see Section 7).

In addition, the Data Protection Act contains specific rules on disclosure of consumer-related personal data to third parties or use of such data on behalf of third parties for the purpose of marketing. The disclosure or use of such data for that purpose is subject to the consumer’s prior explicit consent. However, the disclosure or use of such data may take place without consent, if the disclosure/use relates to general customer data which form the basis for classification into customer categories, provided that (i) the rule of balancing of interests justifies such disclosure/use (please see Section 7(f)) and (ii) the data controller observes the objection procedure.

Thus, the entity must - prior to any disclosure or use of data - check the Central National CPR Register for markings, e.g., whether the consumer in question has filed a statement to the effect that he does not wish to be contacted for the purpose of marketing activities. If the consumer has not given such information to the CPR Register, the entity must inform the consumer about the right to object to the intended disclosure/use in a clear and intelligible manner. The consumer must also be granted an opportunity to object to the disclosure/use in a simple manner within a period of 14 days.
The data may not be disclosed/used until the time limit for objecting has expired.

The entity may not demand any payment of fees in connection with objections.

In Denmark, direct marketing is also regulated by other legislation. Pursuant to the Danish Marketing Practices Act, an entity may not contact anyone (e.g. consumers, other companies, public bodies etc.) by electronic means (e.g., e-mail, text messages, MMS etc.) for purposes of direct marketing without their prior, explicit consent. A very narrow exemption from this rule relates to situations where the person in question, through earlier contact to the entity, has given his contact information when purchasing good or services. Under these circumstances, the entity may communicate marketing messages, but only with regard to the same types/categories of products or services as those purchased by the person in question on earlier occasions. At the same time, the person in question must have a possibility to unsubscribe to such marketing messages, and such un-subscription actions must be without cost and must generally be carried through in an easy manner.

Direct marketing via ordinary mail is allowed subject to prior check of markings in the CPR Register, cf. above.

Moreover, direct marketing to consumers via phone is subject to the consumer’s prior consent, cf. the Danish Consumer Contracts Act. Particular areas are exempted from this requirement, for example insurance contracts and subscriptions for newspapers and magazines.
Egypt

**Hatem Darweesh**  
Cairo  
Tel: +2 02 2461 9301  
hatem.darweesh@bakermckenzie.com

**Hazim Rizkana**  
Cairo  
Tel: +2 02 2461 9301  
hazim.rizkana@bakermckenzie.com
1. Recent Privacy Developments

The Egyptian Constitution was passed in January 2014. Articles 57, 68 and 99 of the Constitution discuss the issue of privacy. Specifically, Article 57 states that "private life is inviolable, safeguarded and may not be infringed upon. Telegraph, postal and electronic correspondence, telephone calls, and other forms of communication are inviolable, their confidentiality is guaranteed and they may only be confiscated, examined or monitored by causal judicial order, for a limited period of time, and in cases specified by the law. The state shall protect the rights of citizens to use all forms of public means of communication, which may not be arbitrarily disrupted, stopped or withheld from citizens, as regulated by the law."

Furthermore, Article 68 provides that "information, data, statistics and official documents are owned by the people. Disclosure thereof from various sources is a right guaranteed by the state to all citizens. The state shall provide and make them available to citizens with transparency. The law shall organize rules for obtaining such, rules of availability and confidentiality, rules for depositing and preserving such, and lodging complaints against refusals to grant access thereto. The law shall specify penalties for withholding information or deliberately providing false information. State institutions shall deposit official documents with the National Library and Archives once they are no longer in use. They shall also protect them, secure them from loss or damage, and restore and digitize them using all modern means and instruments, as per the law."

Lastly, Article 99 stipulates that "any assault on the personal freedoms or sanctity of the life of citizens, along with other general rights and freedoms guaranteed by the Constitution and the law, is a crime with no statute of limitations for both civil and criminal proceedings. The injured party may file a criminal suit directly. The state guarantees just compensation for those who have been assaulted. The National Council for Human Rights shall inform the prosecutor's office any violation of these rights, and also possesses the right to enter into an ancillary civil lawsuit on the side of the injured party at its request. This is as specified within the law."

2. Emerging Privacy Issues and Trends

There are no emerging privacy issues or trends.

3. Law Applicable

In general, there are no data protection laws per se in Egypt. However, individual privacy is protected under the Egyptian Constitution in addition to miscellaneous provisions in different legislations such as:

- the Egyptian Labor Law No. 12 of 2003
- the Penal Code
4. Key Privacy Concepts

The Egyptian Constitution provides that the law shall protect the inviolability of the private life of citizens. Correspondence, wires, telephone calls, electronic correspondence and other means of communication shall have their own sanctity, and confidentiality shall be guaranteed. They may not be confiscated or monitored except by a causal judicial warrant and, even then, only for a definite period and according to the provisions of the law. The Constitution also states that the rights and freedoms of individual citizens shall not be subject to disruption or distraction and that no law shall include a constraint on the practice of such rights and freedoms. Furthermore, the Constitution provides that any encroachment on the rights and freedoms guaranteed in the Constitution shall be considered a crime, for which criminal and civil lawsuits shall not be forfeited by prescription. Victims of such encroachment shall receive fair compensation from the State.

Additionally, the Constitution stipulates that access to information, data, documents and statistics, and the disclosure thereof, is a right guaranteed by the State. However, such disclosure or circulation shall be done in a manner consistent with the protection of the private lives of citizens. The Egyptian Civil Code provides that a person, whose inherent personal rights have been unlawfully infringed, shall have the right to demand cessation of the infringement and compensation for any damage sustained thereby. Whereas, the Egyptian Labor Law states that only those authorized shall have access to review employees’ Personal Data.

The Banking Law stipulates that all bank customers’ accounts, deposits, trusts and safes together with related dealings shall be kept confidential. They may not be reviewed nor may any details be given about them either directly or indirectly except upon written permission from the owner of the account, deposit trust or safe, his successors, anyone to whom all or some of such funds are bequeathed, a legal representative, authorized attorney, or pursuant to a judicial ruling or an arbitral award with such prohibition remaining even if the relationship between the customer and the bank is terminated for any reason.

The Penal Code provides that whoever discloses or facilitates the disclosure of or uses, even privately, a recording or document obtained by any of the following methods – (i) recording or transmitting via private conversations or
on the telephone by any method or (ii) shooting, taking or transmitting a picture of anyone in a private place by any means – without the consent of the concerned party the violator shall be subject to imprisonment. Furthermore, the Penal Code stipulates that any physician, surgeon, pharmacist, nurse or else, who while practicing his profession becomes in the possession of personal secrets and intentionally discloses them without being required to do so by law, shall be punished with imprisonment or a fine.

The Capital Market Law requires brokerage companies to maintain absolute confidentiality of client data and not to divulge any information about them or their dealings to third parties without the prior written approval of the concerned party, and only then within the limits of this approval, with the exception of those cases in which specific information shall be submitted to the Stock Exchange, or regulatory or juridical authorities, as prescribed in the laws. The company shall put procedures in place to ensure that its directors and personnel abide by the obligation to maintain the confidentiality of all data and information. In all cases, the company may not use any data or information for realizing any kind of special gain for itself or any of its other clients without first obtaining the prior written approval from the party to whom the data or information belongs. In addition, the Capital Market Law stipulates that brokerage company employees are prohibited from exploiting insider information gained by virtue of their position or through the nature of their work for their own account or that of a third party, either directly or indirectly. Further, the law states that brokerage company employees are also prohibited from divulging confidential information from client’s accounts and dealings, or carrying out any work liable to prejudice the interest of the dealer or third parties. The dealer shall be banned from dealing in a security if he or she is directly or indirectly cognizant of substantial information related thereto and that such information has not been announced. In such case, the dealer shall be prohibited from giving any other person access to the insider information unless s/he is legally empowered to do so. Finally, the law stipulates that the dealer in the security shall not be considered a user or beneficiary of the insider information if it is established that he dealt with same for reasons other than to gain access, directly or indirectly, to the insider information.

The Communications Law stipulates that the license issued for any entity providing communication services should include details of the licensee’s obligations of ensuring the confidentiality of communications and the clients of the licensee’s private calls, in addition to formulating the necessary rules to ensure same.

The Money Laundering Law stipulates that disclosing any notification, investigation or examination procedures undertaken with respect to financial dealings suspected of involving money laundry or related data to clients, the beneficiary, or non-competent authorities under this Law is forbidden.
a. **Personal Data**

There are no laws specifically addressing the protection of Personal Data in Egypt other than the legislations cited above.

b. **Data Processing**

There are no laws that specifically address and cover the protection of Personal Data with regard to manual and automatic processing.

c. **Processing by Data Controllers**

There are no laws that specifically address processing by data controllers however it is believed that in light of the legal provisions cited above:

- the Labor Law considers an employer a data controller.
- the Banking Law Bank considers officers data controllers.
- the Capital Market Law considers a brokerage company and associated employees data controllers.

The Penal Code considers any physician, surgeon, pharmacist, nurse or other person who while practicing his business or position becomes in the possession of personal secrets as a data controller.

d. **Jurisdiction/Territoriality**

The above cited legislations apply to any person or legal entity having a legal domicile, or local offices or branches in Egypt.

e. **Sensitive Personal Data**

There is no law that specifically addresses sensitive Personal Data other than Article 310 of the Penal Code cited in Section 4 above.

f. **Employee Personal Data**

Employees’ Personal Data addressed under Article 77 of the Labor Law (see Section 4 above) is likely to include Sensitive Personal Data (e.g., health-related information) and non-sensitive Personal Data.

5. **Consent**

a. **General**

There are no laws that specifically address general consent requirements prior to the processing of Personal Data. However, it is recommended that the express consent of any Data Subject be secured in writing.

b. **Sensitive Data**

There are no laws that specifically address Sensitive Data in Egypt. However, it is recommended that the express consent of any Data Subject be secured in writing.
c. **Minors**
There is no law that specifically addresses consent requirements for minors. However, in our view the consent of the guardian of the minor will need to be obtained prior to processing or disclosing data to a third party.

d. **Employee Consent**
There is no law that specifically addresses consent requirements for employees but it is recommended that the employer should obtain their written consent prior to processing or disclosing data to a third party.

e. **Online/Electronic Consent**
Though there is no law that specifically governs online/electronic consent in Egypt, it is believed that electronic consent may be permissible and effective provided that it is properly structured and evidenced.

6. **Information/Notice Requirements**
There is no law that requires an organization to provide Data Subjects with information requirements.

7. **Processing Rules**
There are no specific processing rules in Egypt.

8. **Rights of Individuals**
There are no specific rules regulating the rights of individuals. See Section 4(a).

9. **Registration/Notification Requirements**
There are no requirements for organizations that collect and process Personal Data to register, file or notify the local data authority.

10. **Data Protection Officers**
In Egypt, organizations are not required to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. **International Data Transfers**
There are no laws/rules in Egypt that regulate international data transfers.

12. **Security Requirements**
There are no laws/rules that address security requirements.

13. **Special Rules for Outsourcing of Data Processing to Third Parties**
While there are no laws that specifically address special rules for outsourcing data processing to third parties, it is generally recommended that employers
 notify and obtain prior written consent from their employees before implementing any system for collecting and transferring their employees' Personal Data to third parties. Furthermore, the Capital Market Law requires brokerage companies to maintain client confidentiality, and such requirements can be used as guidelines for other securities companies.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in civil and criminal penalties.

15. Data Security Breach
There is no rule on mandatory breach notification in Egypt.

16. Accountability
Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
Whistle-blower hotlines may be established in Egypt provided that they are in compliance with local laws.

18. E-Discovery
The implementation of an e-discovery system within an organization will not raise privacy issues, provided that, such detection does not disclose personal information. However, if the detection involves disclosure of personal information, then it is recommended that notice be given to all employees that a detection process is in place, an explanation of the purpose for detecting data, and how such detection may have an impact on the employees.

19. Anti-Spam Filtering
There are no laws specifically addressing spam-filtering. But, it is believed that there is no legal obligation for obtaining the consent of individual employees and/or worker representatives before issuing or installing spam-filtering software. However, it is advisable that, as a precautionary measure, the prior consent of employees should be obtained with respect to an employer accessing employees' emails or other private information.

20. Cookies
There are no laws/rules that regulate the use and deployment of cookies in Egypt.

21. Direct Marketing
There are no laws/rules in Egypt that govern direct marketing.
Finland

Hannu Järvinen
Helsinki
Tel: +358 9 6153 3466
hannu.jarvinen@borenius.com

Lauri Leppänen
Helsinki
Tel: +358 9 6153 3423
lauri.leppanen@borenius.com
1. Recent Privacy Developments

New Finnish Information Society Code


The ISC brought along some significant changes, including entirely new concepts, such as “communications providers” and new terminology, such as “traffic data”. The definition of “communications provider” extends the protection of privacy to cover all operators that convey communication as referred to in the ISC. According to the preparatory works for the ISC (HE 221/2013), this would also include confidential messages sent within a service, for example Facebook messaging. The term “traffic data” in the ISC has replaced “identification data”, yet the term still refers to information associated with a legal or natural person used to transmit a message.

Also, contrary to the now repealed Act on the Protection of Privacy in Electronic Communications, the ISC contains an explicit extraterritorial applicability provision in Section 2, under which provisions related to the protection of confidential communication shall apply, if the operator:

1. is established in Finland;
2. is not based in the EU, but the communication network and other equipment to be used in the business operation are located or maintained in Finland; or
3. is not based in the EU, but the services are offered in Finnish or are otherwise targeted at Finland or Finns.

It follows that the applicability of the ISC is not limited to Finnish-based entities, but also sets requirements towards foreign operators.

New Act on Background Checks

A new Act on Background Checks entered into force on 1 January 2015. The new Act implies certain extensions to employers’ right to carry out background checks on their employees, contractors, and job candidates in order to protect important public interests.

Employers may carry out background checks if their employees, contractors or job candidates work in tasks specifically defined in the Act. Like before, the new Act enables carrying out background checks if the employee gains
important knowledge relating to national safety and defence or international relations. However, under this new Act, background checks may also be carried out if the employee has access to information that, if revealed, could seriously damage the economy, the functioning of financial and insurance systems or any business essential for the public.

In addition, the new Act entitles employers to carry out background checks if the employee handles tasks relating to an essential infrastructure or production, for instance in water, energy, food or telecommunications sectors. In practice, companies will be entitled to carry out background checks on employees who are responsible for essential logistical tasks.

The new Act also introduces a register for background checks that will be maintained by the Finnish Security Intelligence Service. The aim of the register is to avoid carrying out unnecessary double checks on persons working short-term in different tasks listed in the Act.

2. Emerging Privacy Issues and Trends

- Prying cases continue to be common in Finland. In the recent years there have been several cases where both patient data and data in the police register have been pried and accessed without authorization. It is common that these cases also gain extensive publicity. In addition to fines, compensations for damages in such data protection offences have been somewhat low, usually in line with the recommendation of EUR 300-800.

- The Finnish Data Protection Ombudsman has released statements on the following areas:
  - The Office of the Finnish Data Protection Ombudsman took part in December 2014 in the open letter addressed to the operators of seven app marketplaces urging them to provide links to privacy policies mandatory for apps that collect personal information. Pursuant to the Data Protection Ombudsman’s guidance, it is already an established rule in Finland that the description of file must be made available to the data subjects prior to the collection of personal data. If personal data is collected in the Internet, the description of file needs to be available also in the Internet.
  - The Data Protection Ombudsman has actively informed Finnish users of the implications of the Costeja case (C-131/12) and how data subjects may request the removal of search results.
  - The Data Protection Ombudsman has given various statements concerning personal data processing in loyalty programmes. Based on these statements it is possible to argue that data processing in loyalty programmes require consent as the legal basis.
3. Applicable Law

The general data protection law in Finland is the Personal Data Act (523/1999) ("PDA"), by which the EU Data Protection Directive (95/46/EC) was implemented in Finland.

http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

The Act on the Protection of Privacy in Working Life (759/2004) ("APPWL") governs data protection in working life, by laying down provisions on such matters as the processing of employees' personal data, the processing of information on drug use, camera surveillance in the workplace and retrieving email messages that belong to the employer.


Under the new Information Society Code (917/2014) ("ISC") relevant provisions on electronic communications and providing information society services are drawn together in one act, repealing many of the previously effective acts on electronic communications. In practice, provisions in relation to several important areas, such as telecommunications, protection of privacy and confidentiality of messages, domain names, electronic marketing and cookies are under this new act.

http://www.finlex.fi/fi/laki/ajantasa/2014/20140917

There are numerous sector-specific regulations, which include data protection related provisions. In particular, the processing of personal data in health care and social welfare is closely regulated. The status and rights of medical patients and clients of social services are protected by the Act on the Status and Rights of Patients 785/1992 and the Act on the Status and Rights of Social Welfare Clients (812/2000).

4. Key Privacy Concepts

a. Personal Data

The PDA defines “personal data” as any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household. Under the Finnish Data Protection Board’s praxis, the PDA also applies to deceased individuals.

b. Data Processing

The PDA includes an extensive definition stipulating that the processing of personal data shall pertain to the collection, recording, organisation, use, transfer, disclosure, storage, manipulation, combination, protection, deletion
and erasure of personal data, as well as other measures directed at personal data. In practice, all measures directed at personal data are deemed as processing of personal data under the PDA.

The PDA does not apply to the processing of personal data by a private individual for purely personal purposes or for comparable ordinary and private purposes.

c. Processing by Data Controllers

Within the meaning of the PDA, a “controller” conceptually refers to one or several persons, corporations, institutions or foundations, for the use of whom a personal data file is set up and who are entitled to determine the use of the file, or who have been designated as controllers by law.

d. Jurisdiction/Territoriality

The PDA applies to the processing of personal data carried out by controllers who are established in Finland or are otherwise subject to Finnish law. Furthermore, the PDA is applied if a controller is not established within the EU but uses equipment located in Finland in the processing of personal data. In such case, the controller shall designate a representative established in Finland.

An exemption has been provided should the equipment be used solely for the transfer of data through the territory of Finland. Based on the preparatory works for the PDA, the mere transfer of data through servers placed in Finland constitutes the use of equipment solely for the transfer of data.

e. Sensitive Personal Data

As a primary rule, the processing of sensitive data is prohibited unless a specific derogation is at hand. Within the meaning of the PDA, sensitive data refers to personal data relating or intended to relate to:

- race or ethnic origin;
- social, political or religious affiliation or trade-union membership of a person;
- a criminal act, punishment or other criminal sanction;
- the state of health, illness or handicap of a person or the treatment or other comparable measures directed at the person;
- sexual preferences or sex life of a person; or
- social welfare needs of a person or the benefits, support or other social welfare assistance received by the person.
The PDA includes a detailed list of exemptions from the prohibition to process sensitive data. The prohibition does not apply:

- if the data subject has given an express consent,
- to the processing of data on the social, political or religious affiliation or trade-union membership of a person, where the person has, by own initiative, brought the data into the public domain,
- if the processing is necessary for safeguarding a vital interest of the data subject or someone else, should the data subject be incapable of giving consent,
- to the processing of personal data necessary for drafting or filing a lawsuit or for responding to or deciding of such lawsuit,
- to the processing of data, which is based on the provisions of an act, or
- when it is needed for purposes of historical, scientific or statistical research.

In addition, the PDA includes specific conditions for the processing of data collected for example in the course of operations of a health care unit, an insurance company or a social welfare authority.

Data processing is limited also with respect to personal identity numbers. In principle, save for limited conditions and exceptions, ID numbers may be processed only on the data subject’s unambiguous consent or by virtue of an act. Also, personal identity numbers should not be unnecessarily included in hard copies printed or drawn up from a personal data file.

**f. Employee Personal Data**

In Finland, the processing of employee personal data is regulated by the Act on the Protection of Privacy in Working Life ("APPWL"), a special statute applied to employment-related personal data processing which is not covered by the PDA.

Under the APPWL, employers may process employee personal data only in accordance with specific conditions. The processing is permitted only insofar as the data is directly necessary for the employee’s employment relationship (necessity requirement).

It is specifically stipulated in the APPWL that no exceptions can be made to the aforementioned requirement of necessity, not even with the employee’s consent.

When collecting employee personal data, the employer shall, as a primary rule, collect the data from the employees themselves. If data is collected from elsewhere, the consent of the employees concerned is required. Exceptions to obtaining this consent are limited only to situations where an authority
discloses information to the employer to enable it to fulfill a statutory duty or when the employer acquires personal credit data or information from the criminal record in order to establish the employee’s reliability.

When data is to be or has been collected from a source other than the employee him/herself, such as when establishing employee reliability, the employer is obliged to notify the employee about the processing and use of the data. The employer must notify the employee of this information before it is used in making decisions concerning the employee.

In addition, the APPWL contains provisions on the processing of employees’ health information. In principle, information concerning an employee’s state of health may be processed only if the information has been collected from the employees themselves or from elsewhere with a written consent from the employees, and if the information needs to be processed in order to pay sick pay or health-related benefits, establish justifiable reasons for absence, assess an employee’s working capacity upon his/her express wish, or if provided elsewhere in the law. Health information may be processed only by those persons who prepare, make or implement decisions concerning employment relationships on the basis of such information.

The collection of personal data during recruitment and during an employment relationship is governed by the cooperative procedure referred to in the Act on Cooperation within Undertakings (334/2007), under which employees or employee representatives need to be consulted prior to initiating data processing activities. The Act on Cooperation within Undertakings is applicable if the company concerned regularly employs at least 20 employees.

5. Consent

a. General

Consent is defined in the PDA as any voluntary, detailed and conscious expression of will, whereby the data subject approves the processing of his/her personal data. The requirement of ‘unambiguity’ underlines the importance of the clarity of the data subject’s expression of will.

Consent does not necessarily have to be in writing and can be given orally provided that the above mentioned requirements are fulfilled. According to the preparatory works for the PDA, even an implied consent could, in certain cases, be sufficient to satisfy the set requirements. The data subject has the right to withdraw his/her consent anytime.

The requirements that a given consent must satisfy shall, in the last resort, be determinable on a case-by-case basis. In case of dispute, the data controller is required to prove that consent exists.
Consent does not supersede the requirement of necessity (see chapter 7 below), meaning that the processing of such data which cannot generally and objectively be considered necessary for the purpose of processing is not justified even if the data subject has given his/her consent.

b. Sensitive Data
A data subject’s express consent constitutes one of the exceptions to the general prohibition to process sensitive data, as stipulated in the PDA. The requirement of ‘express’ consent highlights that the data subject’s consent must be expressed in a precise and active manner. An express consent usually has to be given in writing and must indicate the purpose of the processing of personal data for which the permission has been granted.

c. Minors
The PDA does not include any specific provisions concerning the consent of minors.

d. Employee Consent
The general requirements concerning consent are applicable to employee consent as well. Under the APPWL, employee consent shall not provide an exception to the requirement of necessity, meaning that the employer is only allowed to process personal data directly necessary for the employee’s employment relationship.

Furthermore, the collection of personal data during an employment relationship is subject to cooperative procedures under the Act on Cooperation within Undertakings (334/2007). Thus consent given by employees separately from these procedures can be insufficient.

e. Online/Electronic Consent
A data subject can give his/her lawful consent in the electronic environment. If personal data is collected and processed online, information on the collection and processing must be made available in connection with the online service (e.g., inclusion of a hyperlink to a description of file/privacy notice). If the data subject’s consent constitutes the basis for personal data processing, all necessary information must be made available to the data subject upon giving the consent. The controller must be able to prove that consent has been given.

6. Information/Notice Requirements
When collecting personal data, the controller shall see to it that the data subject can have information on the controller and, where necessary, the representative of the controller, on the purpose of the processing of personal data, on the regular destinations of disclosed data, as well as on how to proceed in order to make use of the rights of the data subject in respect to the processing operation in question. The aforementioned information shall be
provided at the time of the collection and recording of data or, if data is obtained from elsewhere than the data subject and intended for disclosure, at the time of the first disclosure of data at the latest.

The abovementioned required information can, in practice, be provided to the data subject in a description of file, constituting another necessary requirement for the controller. Under the general rules provided in the PDA, the controller shall draw up a description of the created personal data file. The file must indicate the following information:

1. the name and address of the controller and, where necessary, those of the representative of the controller;
2. the purpose of the processing of personal data;
3. a description of the group or groups of data subjects and data or data groups relating to them;
4. the regular destinations of disclosed data and whether data is transferred to countries outside the EU or the EEA; and
5. a description of the principles in accordance to which the data has been secured.

The controller shall keep the description of the file available to anyone. This obligation may be derogated from, if necessary for the protection of national security, defence or public order and security, for the prevention or investigation of crime, or for a supervision task relating to taxation or public finances.

7. Processing Rules

The PDA provides a list of general rules, i.e., principles applying to the processing of personal data. The rules are and concern the following: duty of care, defined purpose of processing, exclusivity of purpose, general prerequisites for processing, data quality, and the drawing of a description of file (discussed in chapter 6 above).

*Duty of care*

Controllers shall process personal data lawfully and carefully, in compliance with good processing practice, and also otherwise so that the protection of the data subject’s private life and the other basic rights which safeguard his/her right to privacy are not restricted without a basis provided by an act. Anyone operating on behalf of a controller, in the form of an independent trader or business, is subject to the same duty of care.
**Defined purpose of processing**

The processing of personal data by the controller must be appropriate and justified. The purpose of the processing of personal data, the regular sources of personal data and the regular recipients of recorded personal data shall be defined before the collection of personal data. The purpose of the processing shall be defined so that the operations of the controller in which personal data is processed are made clear.

**Exclusivity of purpose**

Personal data must not be used or otherwise processed in a manner incompatible with the defined purpose of processing. Later processing for purposes of historical, scientific or statistical research is not deemed incompatible with the original purposes.

**General prerequisites for processing**

The consent of a data subject constitutes the primary justification to process personal data. Should no consent be given, the PDA also enables personal data to be processed, if:

- the data subject has given as assignment for the same, or the processing is necessary in order to perform a contract to which the data subject is a party;
- it is necessary, in an individual case, in order to protect the vital interests of the data subject;
- the processing is based on law;
- there is a relevant connection between the data subject and the operations of the controller, which is based on the data subject being a client or member of, or in the service of the controller or on a comparable relationship between the two (**connection requirement**);
- the data relates to the clients or employees of a group of companies and it is processed within the said group;
- the processing is necessary for purposes of payment traffic, computing or other comparable tasks undertaken on the assignment of the controller;
- the matter concerns generally available data on the status, duties or performance of a person in a public corporation or business;
- the Data Protection Board has issued a permission.

Personal data may be disclosed on the basis of the above mentioned connection requirement only if such disclosure is a regular feature of the operations concerned and if the purpose for which the data is disclosed is not
incompatible with the purposes of the processing and if it can be assumed that the data subject is aware of such disclosure.

**Principles relating to data quality**

Personal data processed must be necessary for the defined purpose of processing (*necessity requirement*). The controller shall additionally see that no erroneous, incomplete or obsolete data is processed (*accuracy requirement*). This duty of the controller shall be assessed in the light of the purpose of the personal data and the effect of the processing on the protection of the data subject’s privacy.

8. Rights of Individuals

The PDA provides data subjects with three fundamental rights, namely the rights of access, *data rectification*, and the *prohibition of processing*. Under the PDA, everyone shall have the right to access data on him/her in a personal data file or to a notion that a file contains no such data, unless this right has been specifically restricted, e.g., on the basis of a compromise to national security, public order or danger caused to the health of someone.

By the request of the data subject, or on its own initiative, a controller shall rectify, erase or supplement erroneous, unnecessary, incomplete or obsolete data from its personal data file. The controller shall furthermore prevent the dissemination of such data. If the controller refuses this request, he must, to this effect, provide a written certificate with which the data subject may bring the matter to the attention of the Data Protection Ombudsman.

A data subject has the right to prohibit a controller from processing personal data for the purposes of direct advertising, distance selling, other direct marketing, market research, opinion polls, public registers or genealogical research.

9. Registration/Notification Requirements

The PDA includes three types of notification requirements. First, the Data Protection Ombudsman shall be notified of all automatic data processing. There are several exceptions to this rule and, in practice, most data processing does not require notification. General notification applies to, for example, data processing for direct marketing purposes and when outsourcing the processing of personal data.

Second, data controllers shall notify the Data Protection Ombudsman regarding personal data transfers outside the EU/EEA. There are several exceptions to this rule and, in practice, most international data transfers do not require notification, as there is no obligation to notify the Data Protection Ombudsman e.g., when using the European Commission’s standard contractual clauses or when the company is Safe Harbour certified.
Third, the PDA stipulates that anyone engaged in credit data activity or carrying out debt collection or market or opinion research as a business, or operating in recruitment, personnel assessment or computing on behalf of another, or using or processing files or personal data in this activity, shall notify the same to the Data Protection Ombudsman.

The notification process is not an authorisation process. Therefore the data controller is always responsible for the lawfulness of its data processing regardless of the notification.

10. Data Protection Officer

Finnish data protection laws do not include a general obligation as regards the appointment of Data Protection Officers. There are, however, certain specific requirements in the health care sector. The Act on the Electronic Processing of Information of Social Welfare and Health Care Clients (159/2007) and the Act on Electronic Prescription (61/2007) require that, inter alia, providers of social welfare or health care services must appoint a Data Protection Officer for monitoring and supervision duties.

11. International Data Transfers

The PDA does not include any special restrictions with respect to the transfer of data within the EU/EEA. Personal data may be transferred outside the EU/EEA only if the country in question guarantees an adequate level of data protection, determined on the basis of the PDA or the findings of the European Commission.

The PDA provides a list of eight derogations enabling the transfer of data outside the EU/EEA. The abovementioned requirements shall not prevent such data transfer if:

1. the data subject has unambiguously consented to the transfer;
2. the data subject has given an assignment for the transfer, or this is necessary in order to perform a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
3. the transfer is necessary in order to make or perform an agreement between the controller and a third party and in the interest of the data subject;
4. the transfer is necessary in order to protect the vital interests of the data subject;
5. the transfer is necessary or called for by law for securing an important public interest or for purposes of drafting or filing a lawsuit or for responding to or deciding such a lawsuit;
6. the transfer is made from a file from which the disclosure of data, either generally or for special reasons, has been specifically provided in an act;

7. the controller gives adequate guarantees of the protection of the privacy and the rights of individuals by means of contractual terms or otherwise, and the Commission has not found, pursuant to relevant articles of the Data Protection Directive, that the guarantees are inadequate; or

8. the transfer is made by using standard contractual clauses as adopted by the Commission in accordance with the Data Protection Directive.

12. Security Requirements

The PDA requires the controller to carry out the technical and organisational measures necessary for securing personal data against unauthorised access, accidental or unlawful destruction, manipulation, disclosure, transfer, and other unlawful processing. The available techniques, the associated costs, the quality, quantity and age of the data, as well as the significance of the processing to the protection of privacy shall be taken into account when carrying out these measures.

In addition, the PDA includes a secrecy obligation. Anyone who has gained knowledge of characteristics, personal circumstances or economic situation of another person while carrying out measures relating to data processing shall not disclose such data to a third person against the provisions of the PDA.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

The duty of care, i.e., the general processing rule applying to the controller, applies also to any third party who, in the form of an independent trader or business, operates on behalf of the controller. Thus, the third party shall process personal data in accordance with the same principles as the controller (see chapter 7). Before starting the processing of data, the third party shall provide the controller with appropriate commitments and other adequate guarantees of the security of data. In practice, compliance with these requirements is ensured contractually between the controller and the third party to whom data processing activities are outsourced.

Furthermore, the outsourcing of data processing requires a notification to the Data Protection Ombudsman, should the third party process personal data on behalf of the data controller.

14. Enforcement and Sanctions

The Finnish Penal Code (39/1889) provides criminal sanctions for personal data offence and breaking into a personal data file.
A person who intentionally or with gross negligence fails to comply with the provisions of the PDA shall be sentenced to a fine for a personal data violation, provided that a more severe penalty is not provided in another act.

A controller is liable to compensate for the economic and other loss suffered by the data subject or another person as a result of the processing of personal data in violation of the PDA.

The Data Protection Ombudsman may order the controller to enforce the data subject’s right of access or to rectify an error.

The Data Protection Board may, at the request of the Ombudsman, give an order prohibiting the processing of personal data in violation of the PDA, compelling a person to remedy an instance of unlawful conduct or neglect, ordering the operations pertaining to a file to be ceased or revoking its permission for processing granted earlier.

15. Data Security Breach

Finnish data protection laws do not impose a general obligation to report data security breaches to a governmental body. However, in relation to specific industries and entities, special regulation exists. First, telecommunication operators are required by law to notify the Finnish Communications Regulatory Authority (“FICORA”) of violations of information security and information security threats. Also, identification service providers are required by law to report severe risks and threats to their data security to FICORA and to the Finnish Data Protection Ombudsman, when the risk or threat concerns personal data. Finally, financial service institutions, e.g., credit institutions and fund management companies, are required to notify the Finnish Financial Supervisory Authority (“FSA”) under FSA’s standards.

16. Accountability

There is currently no law/regulation/guidance in Finland that mandates data controllers to conduct privacy impact assessments or furnish evidence relating to the effectiveness of their data protection management. Pursuant to the PDA, data controllers are merely obligated to plan their personal data processing activities prior to the collection of the personal data.

17. Whistle-Blower Hotline

The Data Protection Ombudsman has published a guide on the implementation of whistle-blower hotlines in Finland-based companies that must comply with the Sarbanes-Oxley-Act of the United States. No other official guidance has been given addressing other than SOX-based whistleblowing schemes. The Data Protection Ombudsman’s guideline can, however, be used as an interpretative tool when assessing other similar whistleblowing schemes.
In general, whistle-blower hotlines at workplaces are not in conflict with Finnish data protection laws, provided that these systems are designed to comply with the data processing requirements imposed by law, fundamentally the PDA and the APPWL (see Section 4(f)). Upon establishing whistle-blower hotlines, companies should, inter alia, define clearly what types of information may be processed and disclosed therein and limit the data to cover accounting, internal auditing, white-collar crime, and prevention of corruption. The data must be correct and directly related to the employment relationship, and comply e.g., with the requirements for data security, description of file, informing of data subjects, right of access, right of rectification, and so forth.

18. E-Discovery

The ISC allows the employer to access the traffic data of messages (such as the size, aggregate size, type, number, connection mode or target addresses of the messages) if the employer complies with certain detailed requirements. Under ISC, collection of traffic data is allowed for the purposes of preventing and investigating potential misuses of the employer’s IT systems or unauthorized disclosure of the employer’s business secrets. As a general rule, data may only be processed with the help of an automatic search function that may be based on the size, aggregate size, type, number, connection mode or target addresses of the messages.

The employer must inform employees beforehand about such monitoring through a cooperative procedure. A prior notification must also be submitted to the Finnish Data Protection Ombudsman. Finally, the employer must draw up a report of the manual processing of traffic data including detailed information on the processing. Companies must also annually notify the Data Protection Ombudsman of any manual processing of traffic data.

19. Anti-Spam Filtering

Messages and identification data may be processed to the extent necessary for the purpose of ensuring information security as provided by the ISC. Such allowed measures include automatic analysis of message content, automatic prevention or limitation of message conveyance or reception and automatic removal of malicious software posing a threat to information security from messages.

20. Cookies

Under the ISC, a service provider may save cookies or other data concerning the use of a service in the user’s terminal device, and use such data if the user has given his/her consent thereto and the service provider gives the user comprehensible and complete information on the purposes of saving or using such data. Implied consent through the use of browser settings is compliant under the ISC and under the Finnish Communications Regulatory Authority’s (“FICORA”) guidance.
The provision above does not apply to any storage or use of data intended solely for the purpose of enabling the transmission of messages in communications networks or which is necessary for the service provider to provide a service that the subscriber or user has specifically requested.

The aforementioned storage and use of data is allowed only to the extent required for the service, and it may not limit the protection of privacy any more than is necessary.

21. Direct Marketing

Pursuant to the PDA, a data subject has the right to prohibit the controller from processing personal data for the purposes of direct marketing. A natural person must be able to prohibit such forms of direct marketing easily and free of charge.

Under the ISC, direct marketing by means of automated calling systems, fax, or email, or text, voice, sound or image messages may only be directed at natural persons who have given their prior consent. A service provider or a product seller may use natural person’s customer contact information that it has obtained in the context of an earlier sale in direct marketing of its own products of the same product group and of other similar products. The customer shall be clearly and extensively notified of the possibility to prohibit such use of contact information at the time when it is collected and in connection with any marketing message.

Direct marketing to legal persons is allowed if the recipient has not specifically prohibited it. Any legal person shall be allowed the opportunity to prohibit the use of its contact information in direct marketing easily and with no separate charge and be given clear notification of this possibility.
France

Magalie Dansac
Paris
Tel: +33 1 44 17 59 82
magalie.dansac@bakermckenzie.com

Idriss Kechida
Paris
Tel: +33 1 44 17 59 08
idriss.kechida@bakermckenzie.com

Denise Lebeau-Marianna
Paris
Tel: +33 1 44 17 53 33
denise.lebeau-marianna@bakermckenzie.com
1. Recent privacy developments

a. New regulations

*Implementation decree of the French Military Program Act*

On 24 June 2015, the new French Intelligence Law was adopted amid fierce debates on the balance between these new provisions and individual’s fundamental democratic rights.

In essence, the Intelligence Law provides French Intelligence Services (as well as other services from the Defense, Home Office, Economy, Budget and Customs ministries, as identified in a forthcoming Decree) with increased powers, including tapping phones, reading emails, setting up hidden cameras or microphones in people’s home, cars or other private areas, bugging electronic devices and using IMSI catchers.

In addition, telecom operators, internet access services providers as well as hosting providers may be required (i) to allow the authorities to access, in real-time, connection data relating to individuals who have been identified by the intelligence services as posing a threat, and (ii) install on their network, automatic processing equipment (so-called “black boxes”) aimed at, through the use of algorithms processing connection data, at searching for patterns that may reveal terrorist threats.

Failure to allow the collection of such connection data or to communicate the information may be sanctioned for up to two years of imprisonment and a fine of up to 150,000 Euros (multiplied by 5 for legal entities). In addition, disclosing the existence and implementation of the above mentioned operations may result in one year of imprisonment and a fine of 15,000 Euros (multiplied by five for legal entities). The Intelligence Law also doubles up the fines for various hacking operations.

The actual implementation of many of these new provisions will require that a number of decrees be issued, which is likely to occur by the end of this year for most of them. Until such decrees are issued, the existing intelligence framework will continue to apply (until 31 March 2016 at the latest).

*Draft bill on digital technology*

In October 2014, the French government launched a national consultation on digital technology, which will be implemented under the aegis of the French Digital Council (Conseil National du Numérique). This consultation aims to help in the drafting of a bill regarding digital issues.

Eventually, two different draft bills should be published within the upcoming weeks: the first would focus on individuals’ rights (including data privacy) issues while the second would emphasize the economic aspects of innovation and digital technology.
These bills are not yet accessible to the public. Based on press articles, the privacy-related draft bill would provide the following:

1. The powers of the CNIL will be extended, as it would have to be consulted for every draft bill or decree related to data protection and processing. In addition the CNIL would be entitled to impose fines of up to 3 millions Euros or 5% of the global annual turnover for companies (instead of 300,000 Euros), as well as to require compliance with the French Data Protection Act 1978 within 24 hours (instead of 5 days).

2. Collective action in order to impede an infringement to the French Data Protection Act would be allowed.

3. The fact that collected data concerns a person under 18 would be considered a legitimate reason to stop the data processing.

4. Internet users would be entitled to give instructions as to their data in case they pass away and to designate a person who may require the deletion of the deceased person’s personal data from websites and social networks.

b. News from Authorities

Adoption of Simplified Standard n°57 by CNIL

The CNIL has adopted simplified standard n°57 (deliberation n° 2014-474) on processing of personal data in connection with monitoring and recording employee telephone calls in the workplace. Simplified standards allow for a streamlined and simplified self-declaration of compliance, as long as the data processing complies with the conditions set forth in said standard. To benefit from this simplified declaration n°57, recordings can only be undertaken if they follow one of these purposes: employee training, employee performance reviews and improvement of service quality. Simplified standard n°57 applies to both public and private institutions, and only allows data processing operations that involve monitoring and recording of employee telephone calls on a periodic basis, to the exclusion of any recording on a permanent or systematic basis. Also excluded are any recordings with the purpose of collecting sensitive data, any audiovisual recording, or any record linkage with data capture on employees’ computers. Data from the recording must be deleted no later than 6 months after such recording, while data from the analysis of the recording must not be kept for a period exceeding one year. Access to recorded data and related analysis must be secured through appropriate technical and organizational measures. Transfers may occur subject to appropriate EU Commission contractual clauses or Safe Harbor Certification or BCRs.
CNIL’s annual activity report for 2014

On 16 April 2015, the French Data Protection Authority (the “CNIL”) published its Annual Activity Report for 2014 summarizing its various accomplishments in 2014, as well as the major challenges and topics that the CNIL will consider in 2015.

The Report notably provides figures on the numbers of complaints, investigations and sanction processes conducted in 2014:

- Of the 5,825 complaints received, 39% relate to e-reputation issues (e.g., deleting online content, fake online profiles, etc.), 16% relate to marketing issues (e.g., marketing email opt-out, retention of banking data, etc.), 14% to labor-related issues (e.g., video surveillance), and 12% to bank/credit issues (e.g., registration on the incidents payment file).

- Of the 421 inspections which were conducted in 2014, 88 of those were targeted at video surveillance and 58 were operated online, in accordance with the new powers granted to the CNIL by the Hamon law of 17 March 2014. 62 notices (warning) have been addressed, but only 18 sanctions were pronounced and among these sanctions, 11 have been published.

CNIL’s new program of control for 2015

On 25 May 2015, the CNIL revealed its intention to remain very active in exercising its controls by planning to conduct 550 controls in 2015 (whereas last year, the number of controls was at 421).

CNIL’s controls are generally carried out as follows (i) 40% stem from its own initiatives based on news released in the press (ii) 28% from its annual program of control (iii) 24% from complaints and (iv) 8% from other items.

Of the 550 controls planned for 2015, the CNIL will proceed to conduct 200 online controls on site and 350 controls on site, in particular 25% of them will be conducted on video protection and video surveillance systems.

The focus of CNIL controls will be on newly implemented technologies which form part of a French consumer’s day-to-day life, including: (i) payment that use NFC technologies, (ii) connected objects used for personal purposes, (iii) national file containing driver’s licenses, (iv) data processing implemented by companies to manage psychological risks and (iv) review of how Binding Corporate Rules (BCRs) are effectively implemented, which calls on companies to be prepared to demonstrate that BCRs are effectively being implemented.

Websites that target the youth are also under CNIL scrutiny which will particularly review the conditions of information and age control mechanisms.
French administrative court confirms CNIL decision sanctioning violation of “right to be forgotten” by online case law database

On 23 March 2015, the Conseil d’Etat, the highest administrative court in France and the court of appeal for CNIL’s decisions, confirmed a CNIL decision sanctioning a violation of the right to oppose the processing of personal data by an online case law website, lexeek.com, grounded on article 38 of the French Data Protection Act (“FDPA”) which allows relief for failure to delete or anonymize data within two months upon request by an aggrieved individual.

The website had posted legal decisions containing the names of four plaintiffs contrary to the CNIL’s 2001 recommendation that case law made available on legal databases should be anonymized. In addition, the website had further failed to delete or anonymize the decisions in question despite the individuals’ request to do so. The CNIL imposed an administrative fine amounting to EUR 10,000 after having served a formal notice on the website to comply with the individuals’ request of opposition.

The decision also comes as a confirmation that a website publisher that organizes, references and makes available legal decisions online is deemed to act as data controller over any personal data contained in such decisions, despite not being the original author of such decisions. Finally, though the argument was not raised in the Conseil d’Etat proceedings, the decision shows that the balance is ever-more tipped in favour of the “right to be forgotten” when balanced against the “right to information,” which might have justified publishing named decisions on the Internet for public information purposes.

CNIL’s investigative powers strengthened by online control

The powers of the CNIL have been strengthened by the new French consumer law published on March 18, 2014. Whereas its investigative powers were limited to three main procedures, namely onsite inspections that allow the CNIL to inspect hardware and software storing personal data, offsite controls that allow the CNIL to verify that data processing practices are compliant by sending injunctions in which it asks for specific documents and hearing procedures that allow the CNIL to summon people involved in data processing to a hearing so it can obtain any relevant information related to the processing above-mentioned, the CNIL has now the power to conduct online controls to prevent and detect any infringements of the French Data Protection Act. However, the CNIL emphasized that the new online investigations are limited to freely accessible online data and cannot be used to bypass security measures implemented to protect websites.
SPAM activities now sanctioned by the French Consumer Protection Agency

The new French consumer law published on March 18, 2014 replaced criminal sanctions that were theoretically applicable for breaches to French anti-spam provisions (Art. L. 34-5 of the French Postal and Electronic Communications Code) but which were very rarely applied (fine of 750 € per breach and/or application of sanctions as set forth in the French Data Protection Act of 1978, as amended) with a new administrative sanction of 15,000 EUR for legal entities, that will now be enforced directly by the French Consumer Protection Agency.

CNIL’s report following its controls on Internet and free Wi-Fi access

The CNIL recently performed a number of investigations aimed at examining data controllers’ (such as in shops, restaurants, hotels, libraries, etc.) compliance with the various French provisions regarding free and public Internet access services. Following these investigations, the CNIL issued in December 2014 its findings on its website which revealed the existence of several breaches.

Based on these findings, the CNIL reminded companies providing such internet access to comply with the various requirements set forth in the French Data Protection Act of 1978, as amended, and in Article L34-1 of the French Postal and Electronic Communications Code. In particular, any free and public Internet access provider must:

1. retain traffic data only which meet the “needs of research, recognition and prosecution of crime” (Article L34-1 of the Code of postal and electronic communications); other data such as the content of exchanged correspondence or information consulted by the users cannot be collected;

2. retain this traffic data for a period of one year only from the date of registration (Article R10-13 Code Post and Electronic Communications) and other data must be regularly removed when no longer needed;

3. provide comprehensive information to service users, given that the control carried out showed that the information provided was largely inadequate or non-existent;

4. refrain from using monitoring tools (e.g., used to ensure the safety of computers, management of invoices, prints, etc.) or parameterize them so as to limit the risk for users’ privacy;

5. include a data protection security and confidentiality clause in their contracts with networks providers, as well as define and implement security measures such as securing access to connection logs, more robust passwords, etc. to ensure data confidentiality;
6. file a normal notification with the CNIL.¹

French Data Protection Authority’s instructions regarding NFC payment cards.

On 19 May 2015, the French Data Protection Authority (“the CNIL”) published straightforward guidelines (“fiche pratique”) on near field communication (“NFC”) payment cards.

In the guidelines, the CNIL reaffirms some principles governing NFC payment cards.

The guidelines state that NFC payment cards can only be used for payments of a sum lower than EUR 20. For any amount greater than EUR 20, the card holder will have to enter a confidential code. Furthermore, the code will also be necessary when the aggregated amount of payments exceed a certain fixed amount.

The guidelines also state that banks must clearly and precisely inform card holders of the NFC functionality and must provide them with an efficient, user-friendly means to oppose it. To respond to clients’ request not to have an NFC card, some banks have, for instance, offered an NFC-disable function on their website which will be taken into account at the next use of the card in an ATM machine.

The CNIL expressly specifies that if a bank does not accept to disable free of charge and with no condition an NFC function upon a card holder’s request, then the card holder can submit a complaint to the CNIL, which will contact the bank if it has sufficient elements grounding the complaint.

The CNIL also emphasizes the importance of NFC card security in these guidelines. The names of the card holders is not anymore readable through the NFC interface for all cards issued from September 2012. Furthermore, from June 2013, the transaction history is also not readable. Banks must constantly adapt their security measures to guarantee that data in cards are not collected and reused by third parties. The CNIL recommends the application of the recommendations issued by the payment cards security observatory in 2007 and 2009 and to encrypt all the data exchanges in order to prevent any access to the data.

¹ http://www.cnil.fr/linstitution/actualite/article/article/internet-et-wi-fi-en-libre-acces-bilan-des-controles-de-la-cnil/?tx_ttnews%5BbackPid%5D=91&cHash=75163b5edae940123ca93e86d97daebf
2. Emerging privacy issues and trends

a. Social media

*French consumer protection agency’s opinion on unfair clauses in social media*

On December 2014, the French Unfair Terms Commission issued an opinion identifying 46 unfair terms in social media Terms & Conditions. In addition to consumer law issues, the Commission addresses under this opinion a number of privacy and data protection related provisions, which is rather unusual. The Commission’s opinion is not binding but has persuasive authority, creating a presumption that the clauses identified in the opinion are unfair under French consumer protection laws.

Contentious clauses in terms of data protection notably include the following:

- it is misleading to advertise social media platform as a free service, while consumers’ personal data are in fact sold to advertisers.
- Privacy policies that state that IP addresses and browsing habits are not personal data as they diverge from the French legal definition of personal data.
- numerous privacy policies do not define specific purposes for which personal data may be used while French law obliges platform to inform users on the specific purposes for use
- provisions that do not impose a strict duration on the platform’s retention of personal data
- clauses that provide for the transfer of personal data outside the EU but do not give the individual the possibility to provide a specific consent to the transfer or consider the consent as being implicitly provided.
- any provisions allowing the service provider to unilaterally modify its privacy policy without notifying the consumer in advance and giving the consumer an opportunity to terminate the service.

b. Internet Sweep Days

In May 2014, the CNIL, together with 26 of its counterparts in the world, conducted an online audit of more than 1,200 mobile apps. A summary of CNIL’s findings was published on its website on September 16, 2014

---

emphasizing the fact that the data protection information provided to applications’ users is usually insufficient\(^3\).

c. **Cookies Sweep Days**

From 15 to 19 September 2014, the CNIL and its European counterparts carried out an audit of the main European websites in order to assess their practices with regard to cookies and, in particular, their compliance with (i) the requirements set forth in the “Telecom Package”, whereby internet users must be informed and provide their consent to the storage of cookies on their computer prior to accessing the website, and (ii) the December 2013 deliberation issued by the CNIL on this subject\(^4\).

In practice, the CNIL checked the number and type of cookies stored on the Internet user’s computer, the way the information on cookies is conveyed to Internet users, the visibility and quality of the information, the process of obtaining the Internet user’s consent and the consequences for a user refusing cookies.

On 30 June 2015, CNIL eventually issued a statement on its website revealing some figures in this regard:

- 24 on-site controls, 27 online controls and 2 hearings were conducted;
- Generally speaking, CNIL noted that internet users are not sufficiently informed and are not in a position to provide their consent prior to cookies being installed on their equipment; and
- 20 websites were eventually ordered by CNIL to comply with their legal requirements.

3. **Law Applicable**

Data Processing, Data Files and Individual Liberties Act of 6 January 1978 (*Loi informatique et libertés*, or “LIL”),


4. **Key Privacy Concepts**

a. **Personal Data**

LIL applies to the processing of any information (“Personal Data”) which directly or indirectly allows for the identification of an individual (“Data Subject”).


\(^4\) [http://www.cnil.fr/documentation/deliberations/deliberation/delib/300/](http://www.cnil.fr/documentation/deliberations/deliberation/delib/300/)
b. Data Processing

“Processing” is extremely widely defined and covers any operation or set of operations performed on Personal Data including collection, recording, organization, storage, consultation, use, disclosure by transmission and deletion.

LIL applies to both manual and automated data processing.

c. Processing by Data Controllers

LIL applies to persons who determine the purposes for which and the manner in which any Personal Data are, or are to be, processed (“Data Controller”).

d. Jurisdiction/Territoriality

LIL applies to:

- data processing activities carried out by Data Controllers established in France; and/or
- data processing activities carried out by Data Controllers established outside the EU that make use of equipment located in France (other than merely for the purposes of transit).

e. Sensitive Personal Data

LIL prohibits the processing of sensitive Personal Data – that is, Personal Data directly or indirectly relating to racial or ethnic origins, political opinions, trade union membership, religious or philosophical beliefs, health or sexual life. However, sensitive Personal Data can be processed if the purpose of the processing justifies it, and provided one of the following conditions is met:

- the Data Subject has given his or her express (i.e., written) consent subject to certain restrictions;
- the processing is necessary in order to protect the vital interests of an individual, and the Data Subject is unable to express his or her consent (where the Data Subject is physically or legally incapable of giving consent);
- the processing is carried out by churches or religious, philosophical, political or union organizations, for the purpose of keeping records of their members or correspondents;
- the Personal Data in question has been made public as a result of steps deliberately taken by the Data Subject;
- the processing is necessary for the management of legal claims;
- the processing is carried out by a health organization, subject to a duty of confidentiality, and is only undertaken for specific purposes;
• the processing is carried out by the National Institute of Statistics and Economic Studies (“INSEE”) or the Ministry’s services, subject to specific requirements;

• the processing is carried out in the context of medical research;

• the Personal Data has been subject to an anonymization process which has been approved by the CNIL, and the processing is carried out under specific conditions; or

• the processing is carried out in the “public interest” and has been authorized by the CNIL.

Certain Personal Data is subject to specific restrictions or prohibitions:

• the processing/use of social security numbers is restricted to the payment by employers of applicable fees to social security, health and retirement organizations;

• Personal Data relating to criminal records can be collected or processed, but only by judicial authorities in the exercise of their functions; and

• the processing of Personal Data relating to health is subject to specific requirements if carried out in the field of research.

f. Employee Personal Data

LIL does not provide for specific rules with respect to employees’ Personal Data. However, the CNIL has published several recommendations and opinions which apply specifically in the employment context and in particular, in respect of the following matters:

• data collection in the recruitment process;

• monitoring of employees’ activity;

• video surveillance;

• badges;

• use of the National Security Number;

• PABX;

• ethics lines;

• global positioning determination (“geolocalization”); and

• discrimination.

In addition, the CNIL participates in and usually follows the opinions of the Article 29 Working Party (see in particular Section 5(d) below).
5. Consent

a. General
Pursuant to LIL, consent of the Data Subject is one of the requirements for processing Personal Data.

When consent is used as a justification for processing, consent must be informed, specific and unambiguous. The consent must be drafted in French. However, consent is not necessary if the purpose is legitimate, provided that the Data Subject has been informed of the data collection and processing as soon as such operations are made.

b. Sensitive Data
Sensitive Personal Data cannot be processed without the specific and express consent of the Data Subject (see Section 4(e) above for exceptions). Express consent is satisfied by either written consent or by a double-click process, if consent is given over the Internet.

c. Minors
The consent of a parent or guardian is required for individuals under the age of 18 (otherwise, collection would be considered unfair). Further, no information on family or way of life should be collected from a minor as this would be considered excessive vis-à-vis the purpose of collection.

d. Employee Consent
The French Authority does not recognize employee consent in light of the Article 29 Working Party’s opinion on the processing of Personal Data in the employment context, which states that it is misleading for an employer to try to rely on an employee’s consent as it is unlikely to be freely given.

e. Online/Electronic Consent
Electronic consent is permissible and can be effective in France provided that it is properly structured and evidenced.

It is advisable that:

- users are clearly informed in French of the required information without having to use links; and
- users should not be able to access website content without having read and accepted a website privacy policy.

6. Information/Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the
Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; how to contact the privacy officer or other person accountable for the organization’s policies and practices; how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

7. Processing Rules
An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and anonymize the Personal Data whenever possible.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. Registration/Notification Requirements
Organizations that collect and process Personal Data are required to file with the local data authority.

10. Data Protection Officers
There is no requirement for organizations to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers
Transfers of Personal Data from France are permitted to:

- another country within the EU or the EEA;
- Canada (under certain circumstances);
- Switzerland;
- Argentina;
- Guernsey;
- the Isle of Man;
- Jersey;
- Faeroe Islands;
• Andorra;
• Israel;
• Uruguay;
• New Zealand; and
• recipients established in the US to the extent that they have chosen to sign up to the Safe Harbor arrangement are generally permitted without the need for formal approval.

Transfers to other countries, or to recipients in the US who have not chosen to sign up to the Safe Harbor arrangement, are prohibited unless:

• the data exporter and the data importer enter into a data transfer agreement providing for adequate protection of the data transferred; or
• the Data Subject is not an employee (and the transfer does not relate to employee data), and has previously given his or her unambiguous, informed and express consent.

When the transfer is authorized through the execution of a data transfer agreement based on unmodified EC model clauses, since 2010, the CNIL does not require the submission of the agreement for validation.

The CNIL recommends the use of data transfer agreements based on unmodified versions of the model contractual clauses approved by the European Commission (either 2001 model or 2004 model) for transfers from a Data Controller to a Data Controller or from a Data Controller to a Data Processor (new model 2010).

BCRs may also be accepted, and the CNIL encourages large multinational companies to implement BCRs to secure transfers of data outside the EU as an alternative to the execution of data transfer agreements. In 2008, the Article 29 Working Party issued three guidelines in order to help Data Controllers draft their own BCRs. BCR clubs have been formed to inform the companies in specific sectors on how to implement BCRs, and the CNIL offers assistance with their implementation. To facilitate the process, there is a mutual recognition system whereby the Data Controller chooses a leading data privacy authority ("DPA") in Europe that will notify all other concerned DPAs of the BCR project and obtain automatic validation of the project.

The CNIL has made available on its website a report on the protection and transfer of Personal Data in the context of outsourcing projects. CNIL offers pragmatic solutions to assist companies with the transfers of Personal Data made outside the EU.
12. Security Requirements
Organizations are required to take steps to: ensure that Personal Data in their possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and are required to comply with sector specific requirements. Organizations may be held liable together with third party providers in case of breach by the latter.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings, and/or private rights of action.

15. Data Security Breach
On 24 August 2011, the French Government adopted an Ordinance (articles 38 and 39 of Ordinance n°2011-1012) which implemented a new security breach notification procedure under the French Data Protection Act.

At this time, only providers of public electronic communications services were covered, i.e. telecommunications providers (e.g., mobile or land communications providers), Internet access providers and voice over IP service providers (“Provider”).

A data security breach is defined broadly as “any security breach that results accidentally or in an illicit manner in the destruction, loss, alteration, disclosure or unauthorized access to personal data which are processed in the context of the supply to the public of electronic communications services”.

The Provider must immediately report the data breach to the CNIL. If the data breach may affect the privacy or the personal data of individuals, the Provider must also inform the affected individuals. The Provider should also maintain an inventory of security breaches including the facts surrounding the breach, its effects and the remedial action taken. This inventory should be at the disposal of the CNIL.

There is an exemption to the notification of individuals affected by the breach if the CNIL acknowledges that appropriate protective measures have been implemented to “scramble” the data so that unauthorized persons having accessed the data may not - in fact - read the data. If the Provider does not
demonstrate that such measures have been implemented, the CNIL, having
considered the likely adverse effects of the breach, may require the Provider
to notify the relevant individuals.

An organization that is involved in a data breach situation may be subject to
an administrative fine, penalty or sanction, civil actions and/or class actions, or
a criminal prosecution.

16. Accountability
Organizations are required to furnish evidence relating to the effectiveness of
the organization’s privacy management program to privacy regulators upon
request.

17. Whistle-Blower Hotline
The Data Controller must obtain the CNIL’s authorization prior to
implementing a whistle-blower hotline.

To simplify formalities, companies may use a fast-track procedure known as
Single Authorization AU-004, provided that the system complies with the
requirements of the CNIL’s decision “AU-004”.

On 14 October, 2010, the CNIL adopted decision no. 2010-369 that modifies
its single authorization AU-004, by reducing the scope. As such, a whistle-
blowing hotline may be used only to comply with: (i) a statutory or regulatory
obligation under French law; (ii) section 301(4) of the US Sarbanes-Oxley law,
or (iii) the Japanese “Financial Instrument and Exchange Act” of 6 June 2006,
also called “Japanese SOX”. Only facts relating to serious risks to the
company in the areas of accounting, financial audit, bribery, banking and the
fight against anti-competitive practices within the concerned organization can
be collected and filed by the organization in charge of handling the reports.

Finally, a Data Controller may not benefit from the fast track Single
Authorization AU-004 if the hotline is used to report any other matters
including where the vital interests of the company or its employees’ physical
or mental integrity are at stake.

18. E-Discovery
When implementing an e-discovery system, an organization may be required
to obtain the consent of employees if the collection of Personal Data is
involved. The organization will be required to advise employees of the
implementation of such system, the monitoring of work tools and the storage
of information.
19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to: inform employees of monitoring policies being implemented in the workplace; give employees the opportunity to opt out from the spam-filtering solution; and give employees the opportunity to review the isolated emails designated as spam.

20. Cookies

The use of cookies must comply with data privacy laws. As such, consent of Data Subjects may have to be obtained before cookies can be used and deployed.

Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. Consent of the Data Subject must be obtained for a specific activity. Bundled consent is not considered valid consent.
Germany

Julia Fitzner
Munich
Tel: +49 89 55238 135
julia.fitzner@bakermckenzie.com

Wolfgang Fritzemeyer
Munich
Tel: +49 89 55238 154
wolfgang.fritzemeyer@bakermckenzie.com

Daniel Krone
Munich
Tel: +49 89 55238 135
daniel.krone@bakermckenzie.com

Benjamin Lotz
Munich
Tel: +49 89 55238 261
benjamin.lotz@bakermckenzie.com

Holger Lutz
Frankfurt
Tel: +49 69 29908 508
holger.lutz@bakermckenzie.com

Michael Schmidl
Munich
Tel: +49 89 55238 211
michael.schmidl@bakermckenzie.com

Matthias Scholz
Frankfurt
Tel: +49 69 29908 203
matthias.scholz@bakermckenzie.com

Matthias Scheck
Munich
Tel: +49 89 55238 135
matthias.scheck@bakermckenzie.com

Michaela Weigl
Frankfurt
Tel: +49 69 29908 508
michaela.weigl@bakermckenzie.com

Julia Wendler
Munich
Tel: +49 89 55238 261
julia.wendler@bakermckenzie.com
1. Recent Privacy Developments

Law on IT-Security

In July 2015 the IT Security Act came into effect. The IT Security Act shall improve the security of information technology systems.

The IT Security Act strengthens the authority of the Federal Office for Information Security (BSI) as the central agency for IT security and expands the investigative authority of the Federal Criminal Police Office in the field of cyber crime.

It also defines requirements for the IT security of critical infrastructure, which includes systems that provide vital services related to information technology, telecommunication, energy, traffic regulation, transport, health, water, food supply, finance and insurance. Operators of critical infrastructural systems will be required to meet minimum standards for IT security and to report significant IT security incidents to the BSI.

Furthermore, the IT Security Act contains stricter requirements for providers of telecommunication and telematic services, which will have to offer state-of-the-art security. Telecommunication companies will also have an obligation to notify their customers if a security breach occurs.

Guidance of the “Düsseldorfer Kreis” on video surveillance/CCTV

In February 2014, the Düsseldorfer Kreis, an association comprising of the 16 Data Protection Authorities in Germany, issued guidance on video surveillance affecting both publicly accessible and non-publicly accessible areas. In order to monitor an area by implementing CCTV one has to meet the requirements of Sec. 6b FDPA, Sec. 28 FDPA and, in case employees are subject to video surveillance, Sec 32 FDPA. By elaborating on these provisions the Düsseldorfer Kreis establishes the following key requirements for conducting legally permissible video surveillance:

- Video surveillance of a publicly accessible area is only permitted in so far as it is necessary, (1) to exercise the right to determine who shall be allowed or denied access or (2) to pursue legitimate interest for precisely defined purposes, and if there are no indications that the data subject’s legitimate interests prevail;
- Video surveillance must be strictly necessary, this necessity should be documented in writing by the data controller;
- Video surveillance must not monitor an individual permanently;
- Sensitive areas have to be exempt from video surveillance;
Data subjects must be clearly informed about the monitoring, whereas employees should be informed accordingly in a separate data protection notice.

Video surveillance footage shall be deleted within the maximum retention period of 48 hours;

Spoken word must not be recorded, and

If employees are subject to video surveillance, certain areas accessible to employees must be exempt.

2. Emerging Privacy Issues and Trends

Enforcement actions

In 2014, a German data protection authority held a German health insurance provider and its members of the board responsible for violating German data protection law. The insurance company admitted that its employees have used personal data of potential customers which were illegally obtained from third party resources in order to approach those potential customers and sell their insurance products. The insurance company had already received a warning letter by the Bundesanstalt für Finanzdienstleistungsaufsicht (German Federal Financial Supervisory Authority) in May 2014 for various breaches of data protection provisions, but no fines have been imposed.

The insurance company settled out of court with the data protection authority and agreed on a fine of EUR 1.3 Mio. and undertook to implementing various data protection measures (e.g. appointing 26 staff members exclusively for compliance and data protection tasks); furthermore, on a voluntary basis, the insurance company declared that it will endorse a professorship for research on data protection by providing funds in the amount of EUR 600.000.

3. Law Applicable

The German Federal Data Protection Act (“FDPA”) outlines the general requirements and obligations relating to the collection, processing and use of Personal Data by private bodies and by federal authorities and bodies. For state authorities and bodies, each German state (Bundesland) has its own state data protection act. If there are specific data privacy provisions, in particular sector-specific laws, then the FDPA is generally superseded by such specific provisions and applies only in cases where there are gaps in the law; e.g. the German Telecommunication Act (“TMA”), the Social Act No. 10 for pharmaceutical companies, or the Postal Act for postal services.

With respect to private bodies, the FDPA applies if the private body collects, processes or uses information relating to an individual in data processing systems or in or from non-automated filing systems, unless the information is collected, processed or used solely for personal or domestic activities. From a territorial perspective, the FDPA applies to private bodies located in Germany.
The FDPA is not applicable in so far as a private body is located in another Member State of the EU/EEA, except where the relevant data collection, processing and use is carried out by an establishment in Germany. The FDPA does apply to data collected, processed or used in Germany by a private entity located outside the EU/EEA using, for purposes of processing Personal Data, equipment, automated or otherwise, situated in Germany. In a recent decision of the European Court of Justice (“ECJ”) against a global internet search engine provider located in the US the ECJ held that EU Member State data protection law applies if a legal entity located in the US processes personal data of EU citizens and if a subsidiary of this US legal entity that is located in the EU is involved in the business operations of the US legal entity by providing marketing support, even though this subsidiary was not involved in the actual data processing activates. In the aftermath of this decision, there is a risk that German data protection authorities and German courts apply the FDPA even broader, even if the black-letter law requirements for its application are not fulfilled.

4. **Key Privacy Concepts**

   **a. Personal Data**

   The FDPA applies to the “collection”, “processing” and/or “use” of “Personal Data,” i.e., any information relating to personal or material circumstances of an identified or identifiable individual (“Data Subject”).

   **b. Data Processing**

   “Collection” means the acquisition of Personal Data about the Data Subject.

   “Processing” is extremely widely defined and covers the recording, alteration, transfer, blocking, and erasure of Personal Data.

   “Use” describes any utilization of Personal Data other than Processing.

   **c. Processing by Data Controllers**

   The FDPA applies to any person or body which collects, processes or uses Personal Data on his, her or its own behalf, or which commissions others to do the same (“Data Controller”).

   **d. Jurisdiction/Territoriality**

   The FDPA applies to:

   - Data Controllers established in Germany that collect, process and/or use Personal Data in Germany;
   - Data Controllers established outside Germany but within an EEA Member State that collect, process and/or use Personal Data in Germany through the Data Controller’s German branch; and
Data Controllers established outside the EEA that collect, process and/or use Personal Data by using equipment located within Germany for such purposes (other than merely for the purpose of transit).

Data Controllers established outside the EEA that collect, process and/or use Personal Data within Germany generally have to appoint a representative in Germany.

e. Sensitive Personal Data

The FDPA imposes additional requirements for the collection, processing and/or use of special categories of Personal Data (“Sensitive Personal Data”) - that is, Personal Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or health or sexual life. Specifically, the collection, processing and/or use of Sensitive Personal Data is prohibited unless certain conditions are met, including:

- the Data Controller obtains the explicit consent of the Data Subject (see Section 5(b) below);
- the collection, processing and/or use is necessary to protect the vital interests of the Data Subject or of a third party where the Data Subject is physically or legally incapable of giving consent;
- the data has evidently been made public by the Data Subject;
- the collection, processing and/or use is necessary in order to assert, exercise, or defend legal claims, and there is no reason to assume that the Data Subject has an overriding legitimate interest in excluding the collection, processing and/or use;
- the collection, processing and/or use is necessary for the purposes of scientific research, and the scientific interest in carrying out the research project substantially outweighs the Data Subject’s interest in excluding collection, processing and/or use, and the purpose of the research cannot be achieved in any other way or would otherwise necessitate disproportionate effort;
- the collection is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services and the processing is undertaken by a health professional or person with the equivalent duty of confidentiality as a health professional; or
- the collection, processing and/or use is necessary for the activities of non-profit-seeking trade unions or organizations of a political, philosophical, or religious nature and where the data concerned only belongs to the organizations’ members or persons who maintain regular contact with the organizations in connection with the purposes of their activities.
f. **Employee Personal Data**

Employee Personal Data is likely to include Sensitive Personal Data (e.g., health-related information, religious denomination) and Personal Data.

An employee’s Sensitive Personal Data may generally only be processed with the employee’s explicit consent (as the other conditions that allow for the processing of such data mentioned in Section 4(e) above will usually be irrelevant in a standard employment relationship). Exceptions apply if the collection, processing or use of such data is allowed or required by law. For example, information regarding religious denomination must be processed for church tax deduction (pursuant to relevant tax provisions).

An employee’s Personal Data may be processed by a Data Controller in certain circumstances, including if (i) the processing activities are necessary for the performance of the employment contract (i.e., if they are required for the fulfillment of primary or collateral contractual or pre-contractual duties), or - arguably - (ii) they are necessary to safeguard justified interests of the Data Controller and there is no reason to assume that the employee has an overriding legitimate interest in his Personal Data being excluded from processing or use.

A fallback justification for processing both Sensitive Personal Data and Personal Data in the employment context is the provision of consent by the Data Subject. However, it is debatable whether an employee can validly give his or her consent in an employment relationship (see Section 5(d) below).

5. **Consent**

a. **General**

Consent of the Data Subject is generally not mandatory for the collection, processing and disclosure of Personal Data. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances.

Consent is contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to only cover the previously identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

Although the FDPA does not contain any express language requirement, the concept of informed consent generally requires the information as well as the consent language itself to be in the German language in order to enable the German Data Subject to understand without doubt what they consent to.
Where Data Subjects are sufficiently proficient in English (or in any other language) consent may also be sought in English (or the other relevant language).

If consent is to be given in writing simultaneously with other declarations, special prominence must be given to the declaration of consent. There is a risk that German courts regard consent given in a standard form agreement as invalid unless there is a separate clause and signature line.

b. Sensitive Data

German law recognizes Sensitive Data as a special category of Personal Data. It is subject to additional and special consent requirements. While Sensitive Data may only be collected and processed with the express consent of the Data Subject, Sensitive Data may be processed without obtaining consent in certain prescribed circumstances.

c. Minors

It is debatable whether the ability to consent depends on the ability to understand – i.e., the capacity to understand the consequences of giving consent (prevailing opinion of the German DPAs) or legal capacity. According to the DPAs, depending on the manner, extent, and purposes of the data processing concerned, an ability to understand can be assumed for minors of around 16 years old. Thus, following the DPAs’ opinion, for minors under the age of 16, consent should be obtained from a parent or legal guardian.

According to a recent decision of the German Federal Supreme Court the consent of minors regarding the collection of personal data for marketing purposes in connection with a sweepstake is invalid. The Federal Supreme Court ruled that a public health insurance company illegally exploits the inexperience of minors if it collects a significant amount of personal data for marketing purposes in connection with a sweepstake. According to the Federal Supreme Court, minors are less capable of foreseeing the consequences and disadvantages of their consent to the collection of their personal data.

d. Employee Consent

German DPAs have raised doubts as to whether consent given in the context of an employment relationship can be considered valid. First, DPAs question whether the consent would qualify as voluntary given that the employee may feel forced to consent due to the subordinate nature of his/her relationship with his/her employer. Second, some DPAs argue that consent would be misleading where statutory permission to collect, process, and use Personal Data is available.

e. Online/Electronic Consent

In Germany, electronic consent is permissible and can be effective if properly structured and evidenced. A simple digital signature and/or a simple mouse-click will generally suffice in the context of advertising, “telemedia services” or
if telecommunication services are at issue. Consent given by way of a simple mouse-click is sufficient only if the following conditions are met:

- the Data Subject is given the necessary information relating to the consent (e.g., on the scope of use of the relevant Personal Data);
- there is an unambiguous and deliberate act by the Data Subject expressing consent to the collection, processing or use;
- the consent is logged;
- the text of the consent is accessible at any time by the Data Subject; and
- the Data Subject is enabled to revoke his or her consent for the future at any time.

German DPAs have issued opinions in individual cases where the DPAs have allowed the use of electronic consent outside of the above mentioned areas of law. This more liberal view is in line with the requirements of the FDPA, which only requires written consent unless the circumstances of the individual case warrant a different form (e.g., in an online context where there is a large number of users, obtaining written consent would be regarded as too burdensome).

6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; and where the Personal Data is to be transferred.

7. Processing Rules

An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; Personal Data should be anonymized or pseudonymized whenever possible; Data Subjects should be provided with the option to use a pseudonym or remain anonymous whenever possible; Personal Data should be deleted/ anonymized once the stated purposes have been fulfilled and legal obligations have been met.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the
correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

Though not mandatory, an organization that collects and processes Personal Data may be required to register, with the competent data protection authority. When an organization appoints a data protection officer, it is no longer required to register with the data protection authority. Registration requirements with the data protection authority can therefore be avoided by appointing a data protection officer even if such an appointment is not legally required.

10. Data Protection Officers

In Germany, an organization must appoint a data protection officer if (i) it employs more than 9 persons with automated processing of Personal Data, (ii) 20 or more persons with any other types of Personal Data processing activities, or (iii) it is subject to the prior checking procedure which is required if (a) sensitive data is processed or (b) the processing of personal data is intended to evaluate the data subject’s personality, including his abilities, performance or conduct, unless such data processing activities are covered by a statutory obligation or the data subject’s consent or are necessary to perform a contract with the data subject.

11. International Data Transfers

Transfers of Personal Data from Germany to other EEA countries are generally permitted without the need for further approval provided such transfers would be legal within Germany. The same applies with respect to transfers to Andorra, Argentina, Canada, Faeroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay which are subject to European Commission findings of adequacy in relation to their data protection laws (subject to the fulfillment of certain pre-conditions).

Transfers to the US are permitted where the recipient has registered under the Safe Harbor arrangement, provided the transfers would be legal within Germany and provided that the recipient actually adheres to the Safe Harbor rules. Transfers to the US or any other countries outside the EEA that do not provide an adequate level of data protection are legal if based on unmodified versions of the relevant EU Model Clauses, always provided that the transfer would be legal within Germany. In the above mentioned cases, no DPA notification or approval is required by law.

Any data transfers based on modified versions of the relevant EU Model Clauses or, on a data transfer agreement entirely different from the relevant EU Model Clauses, must be submitted to the competent DPA for approval. The same is true for data transfers based on Binding Corporate Rules from
the following German states: Berlin, Schleswig-Holstein, and North Rhine Westphalia.

Transfers of Personal Data to countries outside the EEA may further take place without additional measures to ensure an adequate level of data protection at the recipient’s end where:

- the Data Subject has validly consented to the transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller, or to take steps at the Data Subject’s request with a view to entering into a contract with the Data Subject;
- the transfer is necessary for the performance of a contract between the Data Controller and a third party in the interest of the Data Subject;
- the transfer is necessary due to important public interest grounds;
- the transfer is necessary for the establishment, exercise or defense of legal claims; or
- the Personal Data is available from a public register (if certain requirements are met).

12. Security Requirements

Organizations are required to take steps to: ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data, and to comply with sector specific requirements. In case of an occurrence of data breach (see Section 15 of this chapter), the outsourcing organization shall be held liable together with the third party provider.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.
15. Data Security Breach

With effect as of 1 September 2009 a statutory security breach notification was introduced in Section 42a FDPA, which resembles a US-type “Security Breach Notification.” The same security breach notification was implemented in Section 15a Telemedia Act.

Pursuant to these rules, companies are now required to report any illegal transfer of or illegal access to the following types of data, or any knowledge thereof obtained by third parties, always provided that such access or transfer would lead to severe adverse effects on the rights or legitimate interests of the relevant Data Subject’s:

- Sensitive Personal Data;
- Personal Data which are subject to professional confidentiality obligations (e.g., confidentiality obligations applicable under statutory law to attorneys, doctors, etc.);
- Personal Data concerning criminal acts or administrative offenses or suspicion regarding the same; or
- Personal Data relating to bank accounts or credit card accounts.

In cases involving a large number of Data Subjects, other public-oriented measures (such as announcements in two nationwide newspapers) may replace the information of the concerned Data Subjects.

The notification obligation does not require that the security breach is committed intentionally or maliciously. It also does not matter if the Data Controller itself, one of its data processors (if any) or a third party causes the security breach. Scenarios for potential security breaches are thus manifold, for example: a hacker breaks into the company’s database; a fraudster gains access to the company’s data processing systems by phishing user passwords; laptops or storage media are lost or stolen; or an e-mail with Personal Data is sent to the wrong recipient.

The security breach notification generally needs to be provided to the competent DPA and all affected Data Subjects. While the notification to the competent DPA has to be made even if the data leakage is not eliminated or in cases of pending criminal prosecution, the notification to the Data Subjects may be withheld until appropriate measures to safeguard the data have been taken and the notification would no longer endanger criminal prosecution.

The notification of the Data Subject should contain a description of the nature of the unlawful disclosure as well as recommendations for measures to mitigate any possible negative effects. The notification to the competent DPA must, in addition, describe any detrimental consequences of the unlawful disclosure as well as the preventive measures to mitigate the negative consequences of the security breach.
If notifying all Data Subjects requires disproportionate efforts, the notification may be replaced by a notification to the general public, e.g., by means of half-page announcements in at least two nationwide newspapers or other measures having a similar effect.

The notification needs to be provided “without undue delay”. This does not necessarily mean that the notification must be provided immediately. Rather, the Data Controller is given some time to examine the facts and to seek legal advice.

A similar security breach notification obligation was implemented in Section 93 para. 3 in connection with Section 109a of the Telecommunications Act with effect as of 3 May 2012. Therefore, all service providers within the meaning of the Telecommunications Act must inform the Data Subject without undue delay of the violation of the protection of Personal Data if it can be assumed that the violation constitutes a serious harm to the rights or legitimate interests. The notification must include at the very least the following information:

- the type of violation of the protection of Personal Data;
- details of contact points, where further information is available; and
- recommendations regarding measures that limit the adverse consequences of the violation of the protection of personal data.

Companies that render publicly available telephony services must, in addition to notifying the Data Subject, inform the Federal Network Agency and the Federal Commissioner for Data Protection and Freedom of Information without undue delay in case of a violation of the protection of Personal Data. Furthermore, those companies must comply with additional requirements.

An organization that is involved in a data breach situation may be subject to a suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions and/or class actions. or a criminal prosecution.

16. Accountability

Organizations in Germany are required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data; furnish the results of the privacy impact assessments to privacy regulators upon request; and furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.
17. Whistle-blower hotline

Whistle-blower hotlines may be established in Germany provided they are in compliance with local laws. In particular, the Data Protection Officer must be involved early on and, if a works council exists, the works council has a co-determination right.

18. E-discovery

When implementing an e-discovery system, an organization may be required to obtain the consent of employees if the collection of Personal Data is involved. In addition, an organization is required to advise employees of the implementation of an e-discovery system, the monitoring of work tools, and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace and give employees the opportunity to review the isolated emails designated as spam. While not mandatory, an organization may be required to give employees the opportunity to opt-out from the spam-filtering solution.

20. Cookies

There are no specific laws/rules that regulate the deployment of cookies but the general laws (especially the German Telemedia Act) apply. Depending on the type of cookie, consent of Data Subjects by active indication may be required before cookies can be used. Please note that some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond or opt-out. An organization may be required to obtain consent for a specific activity. Consent bundled and hidden in T&Cs is not considered valid opt-in consent neither for direct marketing purposes nor in general.
Greece

Vassilis Constantes
Athens
Tel: +30 210 7206900
v.constantes@vlaw.gr
1. Recent Privacy Developments

The Hellenic Data Protection Authority (“HDPA”) and the Hellenic Authority for the Safeguard of Privacy in Communications have issued Joint Act no. 1/2013 whereby providers of public communication services (services of electronic communication or public communication networks) have to comply with the following safety principles:

(a) The data kept by a provider should be of equal quality and should be equally protected and secured as the data included in the network;

(b) Implementation of appropriate organizational and technical measures to secure data and protect them against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access as well as any other form of unlawful processing;

(c) Implementation of appropriate organizational and technical measures to ensure that access to such data is granted only to specifically authorized personnel.

In 2014, HDPA issued the following, among other decisions: (i) ordering private legal entities in several occasions to delete from their files e-mail addresses that have been used for sending spam without the consent of the recipients; (ii) ordering a private legal entity to stop operating a system of geographical tracking down of the company’s cars used by employees; (iii) ordering a hospital to pay a fine of EUR 30,000 and to destroy files and data collected from the CCTV system that was installed and operated contrary to the relevant provisions of the HDPA’s Directive no. 1/2011; (iv) ordering a bank to pay a fine of EUR 75,000 for buying and processing files containing personal data illegally collected for marketing purposes.

Numerous questions have been raised by public institutions regarding the lawfulness of the installation of biometric systems (fingerprints) for the purpose of controlling and monitoring personnel. In response, the HDPA explained that the use of such biometric systems was burdensome and that the processing was disproportionate to the intended purpose since any control over personnel could be effected efficiently and adequately by other alternative means. To this end, the HDPA ruled that the use of such biometric systems for such purpose should be prohibited.

2. Emerging Privacy Issues and Trends

According to HDPA’s press releases in 2014, several lectures have taken place with respect to data protection issues. The basic issues raised in such lectures were the following:

(i) “Biometric systems and protection of personal data” discussing the question whether biometric systems are compatible with the protection of
personal data and what measures are necessary to ensure that the use of biometric technology does not violate the right of privacy.

(ii) “Use of smart devices – security and personal data” discussing the safety and privacy issues that could arise when employees use their private devices for the purpose of having access to corporate applications for the establishment of files, storage and processing of corporate data (Bring Your Own Device, or “BYOD”).

(iii) “Sensitive data and Cloud computing” discussing legal issues arising from the use of Cloud computing for the protection of privacy with emphasis on the relevant EU Regulation under discussion.

(iv) “Transfer of personal data outside the EU on the basis of contractual clauses” discussing the principal characteristics of the contents of such contractual clauses in respect to the process of approving them.

3. Law Applicable

Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (“PIPPD”), as amended and in force today, implementing the Data Protection Directive (95/46/EC).


4. Key Privacy Concepts

a. Personal Data

Pursuant to the definitions provided by PIPPD, “Personal Data” means any information relating to a Data Subject. A “Data Subject” means any natural person, to whom the data refer and whose identity is identified or may be identifiable, i.e., his/her identity may be determined directly or indirectly, in particular by reference to an identity card number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, political or social identity.

b. Data Processing

Pursuant to the definition provided by PIPPD, “Processing of Personal Data” means any operation or set of operations which is performed upon Personal Data by public administration or by a public law entity or private law entity or an association or a natural person, whether or not by automatic means, such as collection, recording, organization, preservation or storage, alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, interconnection, blocking (locking), erasure or destruction.
c. Processing by Data Controllers

PIPPD applies to any person (public administration or by a public law entity or private law entity or an association or a natural person) who determines the purposes and means of the Processing of Personal Data ("Data Controller"). PIPPD also applies to those persons who process Personal Data on behalf of the Data Controller, such as natural or legal persons, public authorities or agencies or any other organizations ("Data Processor").

d. Jurisdiction/Territoriality

PIPPD applies to any Processing of Personal Data provided that such processing is carried out:

- By a Data Controller or a Data Processor established in Greek territory or in a place where Greek law applies by virtue of public international law; or

- By a Data Controller who is not established in the territory of a member-state of the European Union or of a member of the European Economic Area ("EEA") but in a third country and who, for the purposes of Processing Personal Data, makes use of equipment, automated or otherwise, situated on Greek territory, unless such equipment is used only for the purposes of transit through such territory.

e. Sensitive Personal Data

Pursuant to the definition provided by PIPPD, "Sensitive Data" means data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, social welfare and sexual life, criminal charges or convictions as well as membership to societies dealing with the aforementioned areas.

Pursuant to PIPPD the collection and Processing of Sensitive Data is prohibited. Exceptionally, the collection and Processing of Sensitive Data as well as the establishment and operation of the relevant file, is permitted by the HDPA which is granted only if one of the following conditions occur:

- the Data Subject has given his/her written consent, unless such consent was extracted in a way contrary to the law or morality, or if law provides that any consent given may not lift the relevant prohibition;

- Processing is necessary to protect the vital interests of the Data Subject or the interests provided for by the law or by a third party, if the Data Subject is physically or legally incapable of giving his/her consent;

- Processing relates to Personal Data made public by the Data Subject or is necessary for the recognition, exercise or defence of rights in a court of justice or before a disciplinary body;
• Processing relates to health matters and is carried out by a health professional subject to the obligation of professional secrecy or relevant codes of conduct, provided that such Processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services;

• Processing is carried out by a public authority and is necessary for the purposes of (a) national security, (b) criminal or correctional policy and pertains to the detection of offenses, criminal convictions or security measures, (c) protection of public health or (d) the exercise of public control on fiscal or social services;

• Processing is carried out exclusively for research and scientific purposes provided that anonymity is maintained and all necessary measures for the protection of the persons involved are taken;

• Processing concerns data pertaining to public figures, provided that such data are in connection with the holding of public office or the management of third parties’ interests and is carried out solely for journalistic purposes. HDPA may grant a permit only if such Processing is absolutely necessary to ensure the right to information on matters of public interest as well as in the framework of literary expression and provided that the right to protection of private and family life is not violated in any way whatsoever.

Pursuant to PIPPD, the Data Controller is released from the obligation to obtain from the HDPA prior approval for the collection and processing of Sensitive Data, in case:

(a) Processing is carried out exclusively for purposes relating directly to an employment contract or a contract for work or to the provision of services to the public sector and such processing is necessary for the fulfilment of an obligation imposed by law or for the accomplishment of obligations arising from the above mentioned contractual relationships and the Data Subject has been previously informed.

(b) Processing involves clients’ or suppliers’ data provided that such data are neither transferred nor disclosed to third parties. Insurance companies, pharmaceutical companies, credit or financial institutions are not exempted from the obligation of notification. Courts of justice and public authorities are not considered third parties provided that such a transfer or disclosure is imposed by law or a judicial decision.

(c) Processing is carried out by societies, enterprises, associations and political parties and relates to Personal Data of their members or companies, provided that the latter have given their consent and that such data are neither transferred nor disclosed to third parties. Courts of
justice and public authorities are not considered third parties provided that such a transfer or disclosure is imposed by law or a judicial decision.

(d) Processing involves medical data and is carried out by doctors or other persons rendering medical services, provided that the Data Controller is bound by medical confidentiality or other obligation of professional secrecy provided for in the law or code of practice and data are neither transferred nor disclosed to third parties. Courts of justice and public authorities are not considered third parties provided that such a transfer or disclosure is imposed by law or a judicial decision.

(e) Processing is carried out by lawyers, notaries, land registrars and bailiffs or companies formed by the aforementioned and involves the provision of legal services to their clients, provided that the Data Controller is bound by an obligation of confidentiality imposed by law and that data are neither transferred nor disclosed to third parties, except for those cases where it is necessary and it is directly related to the fulfillment of a client’s mandate.

(f) Processing is carried out by judicial authorities or services with the exception of the judicial – public prosecution authorities and authorities which act under their supervision in the framework of attributing justice or for their proper operation needs.

(f) Employee Personal Data

According to PIPPD, if Processing is carried out exclusively for purposes relating directly to an employment or project relationship or to the provision of services to the public sector and is necessary for the fulfilment of an obligation imposed by law or for the accomplishment of obligations arising from the aforementioned relationships and the Data Subject has been notified in advance, the Data Controller is discharged from the obligation to file a notification with the HDPA and also from the obligation to obtain HPDA’s permission for the processing of its employees’ Sensitive Data.

Apart from the above exception, all other requirements set by PIPPD must be satisfied also for the Processing of both employees’ Sensitive and non-sensitive Personal Data.

HDPA, having taken into consideration the various issues arising from the Processing of Personal Data in the employment context and among others, the opinion of the Article 29 Working Party, has issued its Decision No. 115/2001 whereby, HDPA interprets the existing regulatory framework and indicates how the various issues are likely to be considered in future cases that might be brought before it. Decision 115/2001 among others, sets out the principles for the protection of employees’ Personal Data (including those of former employees or candidate employees) as follows:
• the collection and processing of employees’ Personal Data must be carried out with lawful means and in a way that ensures the respect of employees’ privacy, personality and dignity in the working environment;

• the collection and processing of employees’ Personal Data is allowed exclusively for purposes directly connected to the employment relationship and provided that such processing is necessary for the fulfilment of both sides’ obligations arising either from the law or from the employment contract. The purposes for which the processing of employees’ Personal Data is carried out must be clear and definite. Processing of employees’ Personal Data for reasons that do not involve the employment relationship directly or indirectly is prohibited. Employees should be notified in advance of the above purposes of processing and should be able to understand them. Moreover, the giving of consent by the employee cannot legitimise the processing for purposes other than the ones described above;

• Decision 115/2001 specifically mentions that due to the inherent inequality of the parties in an employment contract and to the position of the employee, the requirement of a consent being given freely by the employee, which is a necessary element of permissible processing, can be questioned in the employment context;

• the employees’ Personal Data that are processed should be adequate, relevant and not excessive in relation to the purposes for which they are collected and processed, should not be kept for longer than is necessary for such purposes and should be kept up to date;

• the employees may not waive the rights granted to them under PIPPD and any such waiver is null;

• the exercise of rights provided for by PIPPD can in no way have negative consequences for the employees (such as negative evaluation of the employee or termination of the employment contract);

• decisions by the employer in relation to the conduct or the efficiency of the employees should not be taken exclusively on the basis of an automated processing of Personal Data; and

• Personal Data collected and processed in order to monitor the safe operation of systems in the working environment may not be used for the control of the employees’ conduct.
5. Consent

a. General

“The Data Subject's Consent” (“Consent”) constitutes any free, explicit and specific declaration of will, which is given in a clear way and in full awareness. By such Consent the Data Subject, having been previously informed, agrees that Personal Data relating to him/her may be processed.

The giving of Consent by the Data Subject is required in order for the Processing of Personal Data to be permissible according to the law. In exceptional circumstances however, the Processing of Personal Data may be carried out, even if no Consent has been given by the Data Subject, if the other requirements provided for by PIPPD are met.

Written Consent for the Processing of non-sensitive Personal Data is not required, although Consent in writing is the most practical and safest way to secure compliance with the requirements of the law.

Although PIPPD does not expressly set any language requirements for Consent, on the basis of the above definition of Consent, such Consent must be given in a language that the Data Subject fully understands.

Also, as the giving of Consent presupposes that the Data Subject has been informed about the Processing in advance, in a proper and clear way and is fully aware of the conditions under which he/she gives his/her Consent, it follows that the relevant information should be given to the Data Subject in his/her language or at least in a language that he/she fully understands.

b. Sensitive Data

Where Consent is relied upon to justify the Processing of Sensitive Data, it must be obtained in writing prior to the Processing.

c. Minors

There is no specific regulatory prohibition or any guidance from the HDPA on collection of Personal Data from children. Processing of Personal Data related to minors has to be made under the requirements of the PIPPD. Notification and Consent requirements have to be obtained from the parents exercising the parental care and representing their child in every affair or legal action.

d. Employee Consent

All the requirements set by PIPPD for the giving of Consent by any Data Subject shall equally apply to Consent given by employees. As in all other cases, in the employment context the giving of Consent constitutes the rule for a legitimate Processing of Personal Data.

Nevertheless, as mentioned above, HDPA has acknowledged the possible invalidity of a Consent given in the employment context, due to the fact that the position of the employee may not allow the free giving of such Consent.
However, HDPA has not provided any specific guidelines as to when a
Consent may be considered to have been freely given.

HDPA in Decision No 115/2001, has stressed however that the giving of a
Consent by an employee cannot provide a remedy for non-compliance with
the principles of a legitimate Processing (e.g., consent in relation to
Processing for purposes not connected with the employment contract) and
therefore it generally follows from Decision No 115/2001 that the Consent is
valid when it refers to a Processing of Personal Data for which all the other
requirements of the law are met.

e. Online/Electronic Consent

HPDA issued Directive 2/2011 whereby the requirements are set for the
legitimate granting of Consent by electronic means (“Electronic Consent”) for
the Processing of Personal Data of a subscriber or user by a Data Controller
within the framework of article 11 of Law 3471/2006 on the Protection of
personal data and privacy in the electronic communications sector, i.e., for
effecting communications for the purpose of direct marketing or other
advertising purposes by using communication systems without human
intervention (e-mails, SMS, MMS etc).

6. Information/Notice Requirements

The Data Controller must inform the Data Subject of the following when
Personal Data are collected:

- the identity (name, precise address and telephone number) of the Data
  Controller and of its representative in Greece;
- the purposes of the processing, in a manner that is unambiguous and
easy to understand;
- the Personal Data or categories of Personal Data being processed by the
  Data Controller;
- the recipients or categories of recipients of the Personal Data; and
- the Data Subject’s right of access to the Personal Data and the right to
  object to the processing of Personal Data relating to the Data Subject.

The Data Subject must be informed of any change in the above information
promptly and in any event prior to any further use or processing of the
changed Personal Data.

If Personal Data are disclosed to a third party, the Data Subject must be
informed in writing prior to such disclosure.

When Personal Data are collected directly from the Data Subject, the Data
Controller must provide the information at the time of collection. If Personal
Data are collected from other sources, the Data Subject should be informed
promptly and in any case prior to any further use or processing of the Personal Data.

If the Data Subject gives his /her required Consent or assistance to the Data Controller for the collection of Personal Data, then the Data Subject must receive the above information in writing.

If the Data Subject's Consent is not required for the collection and Processing of Personal Data, the Data Subject must be informed about the Processing in the most appropriate and unambiguous way, so that the Data Subject is freely and adequately informed, e.g., by hanging a notice in the place of business or, by delivering printed material.

The above obligation of the Data Controller to provide information to the Data Subject may be lifted by a decision of the HDPA if the processing of the Personal Data is carried out for purposes of national security or for the investigation of particularly serious crimes or if the registration, purpose of the processing, the recipients and the right of access constitute common knowledge of any diligent citizen.

Without prejudice to the right of access and to the right to object to the Processing of Personal Data, the above obligation to inform the Data Subject does not exist if the Processing takes place exclusively for journalistic purposes and refers to public figures.

No language requirements are stipulated in the PIPPD, however, the relevant information should be given to the Data Subject in the language spoken or at least clearly understood by the Data Subject.

7. Processing Rules

According to PIPPD, the Processing of Personal Data is allowed only if the Data Subject has given his/her Consent. In the specific exceptional cases listed below, Processing is allowed without the giving of Consent:

- if Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; or
- if Processing is necessary for compliance with a legal obligation to which the Data Controller is subject; or
- if Processing is necessary in order to protect the vital interests of the Data Subject, where the latter is physically or legally incapable of giving consent; or
- if Processing is necessary for the performance of a task of public interest or of a task falling within the scope of exercise of public power and performed by a public authority or assigned by the latter either to the Data Controller or to a third party to whom the Personal Data are disclosed; or
• if Processing is absolutely necessary for the purposes of satisfaction of
  the legitimate interest pursued by the Data Controller, or by the third party
  or parties to whom the Personal Data are disclosed, provided that such
  interest obviously overrides the interests and rights of the Data Subjects
  and the fundamental freedoms of the Data Subjects are not offended.

The Data Controller must also ensure that:

• Personal Data are collected in a fair and legitimate way, for specified,
  explicit and legitimate purposes and further processed fairly and
  legitimately in view of those purposes;

• Personal Data are adequate, relevant and not excessive in relation to the
  purposes for which they are processed;

• Personal Data are accurate and up-to-date; and

• Personal Data are kept in a form that allows the identification of the Data
  Subjects to whom such Personal Data refer only as long as it is
  necessary for the purpose for which they were collected and processed.

Processing of Personal Data must be confidential and must be carried out
exclusively by persons supervised and acting only on the basis of instructions
from the Data Controller or the Data Processor. The Data Controller must
select persons with relevant professional skills, who provide sufficient
 guarantees in respect of technical expertise and personal integrity ensuring
compliance with confidentiality requirements.

The Data Controller must implement appropriate organisational and technical
measures to secure data and protect them against accidental or unlawful
destruction, accidental loss, alteration, unauthorised disclosure or access as
well as any other form of unlawful processing. Such measures must ensure a
level of security appropriate to the risks presented by processing and the
nature of the data processed.

In addition to the above, the other requirements set by PIPPD for the
Processing of Personal Data must be complied with.

8. Rights of Individuals

Right of access: A Data Subject has the right to be provided, on request and
without any delay, with information on his/her Personal Data that are
processed by the Data Controller. The information provided by the Data
Controller must be in an intelligible form and include:

• all the Personal Data related to the Data Subject making the request as
  well as their source(s);

• the purposes for which Personal Data are processed;

• the recipients or categories of recipients of the Personal Data;
• the development of the processing during the period from the last notification or information to the Data Subject; and

• the logic involved in an automated processing.

If the Data Controller fails to reply within 15 days or his reply is not satisfactory, the Data Subject may appeal before the HDPA. If the Data Controller refuses to satisfy the Data Subject’s request, the Data Controller must notify his reply to the HDPA and inform the interested party who can then appeal before the HDPA.

A Data Subject has the right to:

• be informed by the Data Controller prior to the processing of his/her Personal Data;

• object in writing to the Processing of his/her Personal Data and receive a response from the Data Controller within 15 days and to have Personal Data rectified, non-transferred, blocked or erased where the Processing of that Personal Data has not been conducted in accordance with the law;

• apply to any competent court for the suspension or non-application of an act or decision affecting him, based solely on automated processing of Personal Data intended to evaluate his/her personality and especially his/her effectiveness at work, creditworthiness, reliability and general conduct;

• to claim full compensation for any material damage suffered as well as for moral damages suffered as a result of a violation of the provisions of PIPPD by any natural person or legal entity; and

• to prevent the Data Controller from using his/her Personal Data for the purposes of direct marketing.

9. Registration/Notification Requirements

The Data Controller is required to file a notification with the HDPA before commencing any manual or automated data processing. The notification requires detailed information including the following:

• the name, or the trade name or distinctive title of the Data Controller as well as his address. If the Data Controller is not established in Greece, or in a place where Greek law applies, the name, or the trade name, or the distinctive title and address of his representative in Greece must also be notified;

• the address where the file or the main equipment supporting the processing is situated;

• a description of the purpose for which the Personal Data included in the file or to be included in the file are processed;
• the kind of Personal Data that are processed or intended to be processed or included or intended to be included in the file;

• the time period during which the processing of the Personal Data is expected to be carried out or the file is expected to be maintained;

• the recipients or categories of recipients to whom the Personal Data are or might be disclosed;

• any eventual transfer of Personal Data to other countries and the purpose of such transfer;

• the basic characteristics of the system and of the safety measures of the file or of the processing; and,

• if the processing falls within the scope of special categories for which the HDPA has determined special processing rules, a declaration that the processing is going to be carried out in accordance with those rules.

The above information is registered in a Register of Files kept by the HDPA. Any modification of the information referred to above must be communicated, in writing and without any delay, to the HDPA.

Pursuant to PIPPD, the Data Controller is released from the obligation to make a notification to the HDPA in case:

• Processing is carried out exclusively for purposes relating directly to an employment contract or a contract for work or to the provision of services to the public sector and such processing is necessary for the fulfilment of an obligation imposed by law or for the accomplishment of obligations arising from the above mentioned contractual relationships and the Data Subject has been previously informed.

• Processing involves clients’ or suppliers’ data provided that such data are neither transferred nor disclosed to third parties. Insurance companies, pharmaceutical companies, credit or financial institutions are not exempted from the obligation of notification. Courts of justice and public authorities are not considered third parties provided that such a transfer or disclosure is imposed by law or a judicial decision.

• Processing is carried out by societies, enterprises, associations and political parties and relates to Personal data of their members or companies, provided that the latter have given their consent and that such data are neither transferred nor disclosed to third parties. Courts of justice and public authorities are not considered third parties provided that such a transfer or disclosure is imposed by law or a judicial decision.
• Processing involves medical data and is carried out by doctors or other persons rendering medical services, provided that the data Controller is bound by medical confidentiality or other obligation of professional secrecy provided for in the law or code of practice and data are neither transferred nor disclosed to third parties. Courts of justice and public authorities are not considered third parties provided that such a transfer or disclosure is imposed by law or a judicial decision.

• Processing is carried out by lawyers, notaries, land registrars and bailiffs or companies formed by the aforementioned and involves the provision of legal services to their clients, provided that the Controller is bound by an obligation of confidentiality imposed by law and that data are neither transferred nor disclosed to third parties, except for those cases where is necessary and is directly related to the fulfillment of a client’s mandate.

• Processing is carried out by judicial authorities or services with the exception of the judicial – public prosecution authorities and authorities which act under their supervision in the framework of attributing justice or for their proper operation needs.

10. Data Protection Officers

PIPPD provides that the processing of Personal Data is carried out exclusively by persons supervised by and acting on the basis of instructions from the Data Controller or the Data Processor. Indirectly, it can be inferred from this requirement that the Data Controller or the Data Processor must appoint specific persons who will undertake the task of Processing Personal Data. There is no provision indicating that the above persons appointed by the Data Controller or the Data Processor should also be notified to the HDPA, although the standard registration/notification form (prepared by the HDPA) requires that the contact details of a natural person nominated by the Data Controller be included therein, for the purpose of providing additional information that may be required by the HDPA.

11. International Data Transfers

Pursuant to PIPPD, transfer of Personal Data is permitted: (a) for member states of the European Union and (b) for a non-member of the European Union following a permit granted by the HDPA if it deems that the country in question guarantees an adequate level of protection. A permit by the HDPA is not required if the European Commission has decided on the basis of the process of article 31, paragraph 2 of Directive 95/46/EC of the parliament and the Council of 24 October 1995 that the country in question guarantees an adequate level of protection in the sense of article 25 of the aforementioned Directive.
The transfer of personal data to a non-member state of the EU which does not ensure an adequate level of protection is exceptionally allowed only following a permit by the HDPA, provided that one or more of the following conditions occur:

- the Data Subject gives his/her consent for the transfer, unless such consent has been extracted contrary to law or morality;

- the transfer is necessary: (a) for the protection of the vital interests of the Data Subject, provided he/she is physically or legally incapable of giving consent; or (b) for the conclusion and performance of a contract between the Data Subject and the Data Controller or between the Data Controller and a third party in the interests of the Data Subject, provided the Data Subject is physically or legally incapable of giving consent; or (c) for the implementation of pre-contractual measures taken in response to the Data Subject’s request;

- the transfer is necessary in order to address an exceptional need and safeguard a superior public interest, especially for the performance of a co-operation agreement with the public authorities of the other country, provided the Data Controller adduces sufficient safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of corresponding rights;

- the transfer is necessary for the establishment, exercise or defence of a right before the Court; or

- the transfer is made from a public register which according to the law, is intended to provide information to the public and which is open to consultation either by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in the law for consultation are fulfilled in the particular case.

The Data Controller shall provide adequate safeguards with respect to the protection of the Data Subjects’ personal data and the exercise of their rights, when the safeguards arise from conventional clauses which are in accordance with the regulations of PIPPD. A permit is not required if the European Commission has decided, on the basis of article 26, paragraph 4 of Directive 95/46/EC that certain clauses offer adequate safeguards for the protection of personal data.

12. Security Requirements

The Data Controller must implement appropriate technical and organisational measures for the safety of the Personal Data and also to protect Personal Data against accidental or unlawful destruction or accidental loss or unauthorised alteration, disclosure or access, as well as any other form of unlawful processing. Such measures must ensure a level of security appropriate to the risks represented by the processing and the nature of the
Personal Data. HDPA proposes that Data Controllers adopt security plans, security policies, disaster, recovery and contingency plans.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

Where the Data Controller outsources the Processing to a Data Processor who is not dependent on the Data Controller, the processing must be carried out under a contract which:

- is made in writing;
- requires the Data Processor to act only on the basis of the instructions of the Data Controller and comply with the security and confidentiality obligations of the law equivalent to those imposed on the Data Controller.

14. Enforcement and Sanctions

**Sanctions** for breach of the Data Controllers’ duties arising from PIPPD:

**Administrative sanctions**

The following administrative sanctions may be imposed:

(a) a warning with an order for the violation to cease within a specified time limit;

(b) a fine ranging from EUR 880.41 to EUR 14,673.51;

(c) a temporary revocation of the permit;

(d) a definitive revocation of the permit; or

(e) the destruction of the file or a discontinuance of the processing and the destruction of the relevant Personal Data.

The sanctions in b, c, d, and e above will only be imposed following an administrative hearing before the HDPA. The sanctions in c, d, and e will be imposed in the case of serious or repeated violation. A fine may be imposed in conjunction with the sanctions in c, d and e above.

**Penal sanctions**

There are various penal sanctions provided for in PIPPD depending on the breach of its provisions. The relevant punishment may be imprisonment from ten days to five years and fines ranging from EUR 2,934.70 to EUR 29,347.03. The penalties are as follows:

(i) any person (or in the case of a legal entity the legal representative(s)) processing Personal Data without a notification to the HDPA (where such notification is required) is punishable with imprisonment of up to three (3) years and a penalty from EUR 2,934.70 to EUR 14,673.51;
(ii) any person (or in the case of a legal entity the legal representative(s)) processing sensitive Personal Data without permission by the HDPA or in violation of the terms and conditions of the HDPA’s permission is punishable with imprisonment of at least one (1) year and a penalty from EUR 2,934.70 to EUR 14,673.57;

(iii) any person (or in case of a legal entity the legal representative(s)) interconnecting files without notification to the HDPA, is punishable with imprisonment of up to three (3) years and a penalty from EUR 2,934.70 to EUR 14,673.57. Any person interconnecting files without the permission of the HDPA (where such permission is required) or in violation of the permission granted, is punishable with imprisonment of at least one (1) year and a penalty from EUR 2,934.70 to EUR 14,673.51;

(iv) any person (or in case of a legal entity the legal representative(s)) that interferes with Personal Data files or takes knowledge of such Personal Data or alters, damages, destroys, processes, transfers, communicates or gives access to such Personal Data to third parties or exploits the Personal Data in any way, is punishable with imprisonment and a fine; or

(v) a Data Controller who fails to comply with the requirements of PIPPD with regard to transfers of Personal Data, is punishable with imprisonment of at least two (2) years and pecuniary penalty ranging from EUR 2,934.70 to EUR 14,673.51.

Where violations under (i) and (v) are due to negligence, the liable person is punishable with imprisonment of up to three (3) years and pecuniary penalty. Furthermore, if such violations were committed in order for the liable person to obtain, for himself or for any other party, an illegal financial benefit or in order to damage a third person, then the liable person is punishable with imprisonment from five (5) to ten (10) years and a pecuniary penalty from EUR 5,869.40 to EUR 29,347.03.

If the breach of certain provisions of PIPPD has created a risk to the democratic constitution or to national security, the punishment may include imprisonment of up to twenty years and a fine ranging between EUR 14,673.51 and EUR 29,347.03.

Civil liability

Any natural person or legal entity who in breach of PIPPD, causes material damage will be liable for damages in full. If damages are non-pecuniary, (e.g., moral damages) compensation may be payable. In the case of moral damages, minimum compensation is set at EUR 5,869.40, unless the plaintiff claims a lesser amount or the breach was due to negligence. Such compensation is awarded irrespective of the claim for damages.
Recent penalties imposed by HDPA for non compliance with PIPPD:

- EUR 50,000 fine imposed on a financial institution due to a failure to safely destruct data files and for violation of data subjects’ right to access their data;
- EUR 30,000 fine imposed on a private company for violation of the data subjects’ right to object;
- EUR 30,000 fine imposed on a financial institution for violation of the obligation to ensure lawful processing of data (processing of non-accurate and not updated data) and data subjects’ right to object;
- EUR 30,000 fine imposed on a company providing telecommunication services for violation of data subjects’ right to object and unlawful interconnection of files;
- EUR 15,000 fine imposed on a private company for violation of data subjects’ right to access their data;
- EUR 10,000 fine imposed for unlawful publication of sensitive data;
- EUR 4,000 fine imposed for violation of data subject’s right to information and,
- Decisions of Greek Civil Courts granting Data Subjects monetary awards ranging from EUR 3,000 up to EUR 15,000 for moral damages caused by the violation of the PIPPD.

15. Data Security Breach

Apart from the principles of confidentiality and security of any Processing set by PIPPD and apart from HDPA’s guidance on security measures, there has been no specific decision or guidance issued by HDPA in relation to specific notification requirements in cases of security breaches.

16. Accountability

We have not been able to trace any law or decision of the HDPA requiring the conduct of privacy impact assessment prior to implementing new information systems for the Processing of Personal Data.

17. Whistle-Blower Hotline

We have not been able to trace any law or decision of the HDPA setting principles or specific requirements for the implementation of whistleblowing schemes in Greece. Therefore, for a whistleblowing scheme to be lawful, it should be in compliance with all the principles and requirements set forth by PIPPD.
18. E-Discovery
When implementing an e-discovery system, a Data Controller is required to inform the users (e.g., employees) and comply with the principles of lawful Processing of Personal Data set by PIPPD.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution a Data Controller is required to inform employees of monitoring policies being implemented and comply with the principles of lawful processing of personal data set by PIPPD.

20. Cookies
The use of cookies must comply with the principles set by PIPPD.

21. Direct Marketing
Pursuant to article 11 of Law 3471/2006 on the Protection of Personal Data and Privacy in the electronic communications sector, “the use of automated calling systems without human intervention, facsimile machines or e-mail for the purposes of direct marketing of goods or services or any advertising purposes may only be allowed in respect of subscribers who have given their prior consent. So a spam which is sent without the prior consent of the recipient is illegal. Exceptionally where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or service, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner to such collection and use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use. Moreover, the practice of sending e-mail for purposes of direct marketing of goods and services disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease shall be prohibited.

In addition, the decision of the HDPA dated 20 January 2000, on the conditions under which the processing of Personal Data for the purposes of direct marketing or advertising is permissible, provides that a free, explicit and specific consent is required, by which the Data Subject, after having been properly informed, agrees in advance to the processing of his/her Personal Data for direct marketing purposes (i.e., an opt in).

In exceptional cases, processing Personal Data for direct marketing purposes is lawful, even if no consent is given by the Data Subject, provided that: (a) such processing is necessary for the purposes of the legitimate interests pursued by the Data Controller; (b) such legitimate interests of the Data
Controller clearly override the interests of the Data Subject; and (c) the fundamental rights and freedoms of the Data Subject are not offended.

In its above decision, the HDPA sets the following conditions under which the above exception (i.e., processing without consent) shall apply:

- the Personal Data comes from directories intended for public access and it is certain that the Data Subjects included therein have given their consent for inclusion in such directories, or comes from publicly accessible sources intended to provide information to the public, provided that the legal requirements for access to such sources have been observed or the Data Subject himself has published his details for marketing or similar purposes;

- the Data Controller has received information from the Registry kept by the HDPA concerning the persons that do not wish for their Personal Data to be included in files of data that are processed for the purposes of promotion of sales of goods or services from a distance and has excluded such persons from his files;

- the Data Controller only keeps the Personal Data that are absolutely necessary for the specific purposes and such Personal Data are solely the name, address and profession of the Data Subjects;

- the purpose of the processing is restricted to advertising or promotion of sale of goods or the provision of services from a distance and is not contrary to good morals.

Further, the above decision of the HDPA provides, among other requirements, that the Data Controller must provide information to the Data Subject at the time of collection and during the first transmission of the Personal Data in accordance with the relevant provisions of PIPPD and the decisions of the HDPA on provision of information to Data Subjects.
Hong Kong

Anna Gamvros
Hong Kong
Tel: +852 2846 2137
anna.gamvros@bakermckenzie.com

Susan Kendall
Hong Kong
Tel: +852 2846 2411
susan.kendall@bakermckenzie.com
1. Recent Privacy Developments

*New Guidance for the Responsible Collection and Use of Biometric Data*

In July 2015 the Privacy Commissioner for Personal Data (“Commissioner”) issued *Guidance on Collection and Use of Biometric Data* (“BD Guidance”). It was released the day before publication of an investigation report by the Office of the Privacy Commissioner (“PCO”) into the collection of fingerprint data by Queenix (Asia) Limited, in which the Commissioner served an Enforcement Notice on Queenix for excessive collection of fingerprint data.

The non-binding guidance recognises both *physiological* (such as fingerprint data, DNA, facial image) and *behavioural data* (such as handwriting, gait) as biometric data. While it may not be reasonably practical to ascertain the identity of an individual from such data alone, when linked with personal data in another database, an individual/data subject can be identified from such biometric data. Therefore this data is considered “personal data”.

The BD Guidance cautioned that the appropriateness of collection varies with the level of sensitivity of the biometric data concerned. Meanwhile, the report made it clear that the PCO considers the collection of biometric data to be a serious issue and unnecessary or excessive collection of such data will not be tolerated.

Both the report and the guidance stressed the importance of carrying out a Privacy Impact Assessment before deciding to collect biometric data. In particular, clients should:

- have strong justification for collecting biometric data;
- ensure that free and informed consent is obtained prior to collection;
- adopt risk minimisation techniques and implement strong controls to protect the data once collected; and
- where possible, use less privacy intrusive alternatives than collecting biometric data.

If such data is collected, the BD Guidance outlined considerations, such as keeping the data in “template” form, only collecting for a lawful purpose and not to be excessive. A number of risk minimisation strategies were also outlined.

Further, data subjects should be provided with a free and informed choice to allow the collection of their biometric data, together with a full explanation of the personal data privacy impact of the collection of such data. The PCO offered guidance on the type of information to be provided, which is similar to the other information requirements for personal data. It includes whether the provision of the biometric data is voluntary or obligatory, consequences of not providing the data, purpose of use, who has access, classes of transfers,
whether the biometric data could be relied upon to take adverse actions against the individual concerned and their rights to request access and correction.

Finally, where data is collected, the BD Guidance sets out a number of requirements in handling such data, including:

- Establishing strong controls for access to, use and transfer of biometric data, including written policy and clear guidance to prevent unnecessary linkage between biometric databases with other systems, transfer or change of the data;
- Regularly and frequently purging biometric data no longer required for the purpose for which it is collected;
- Taking all reasonably practicable steps to ensure data is accurate;
- Not using personal data for a new purpose except with consent;
- Taking all reasonably practicable steps to ensure the biometric data is protected against unauthorised or accidental access, processing, erasure, loss or use having regard to the kind of data and harm that could result;
- Devising policies and procedures setting out clearly the rules and practices in collection, holding, processing and use of biometric data and make them available to data subjects;
- Regular compliance assessments and reviews, as well as proper training, guidance and supervision; and
- If contractors are engaged, adopting contractual or other means to prevent the contractor keeping the data longer than necessary and protection from unauthorised or accidental access, processing, erasure, loss or use.

New Guidance on the responsible use of Drones

In March 2015 the Commissioner updated and expanded its existing guidance on CCTVs to encompass the use of drones, titled Guidance on CCTV Surveillance and use of Drones (“Drones Guidance”).

The Drones Guidance outlined the particular concerns of drones, namely that they are small, portable and mobile, enabling them to track an individual’s activities more persistently over time and in a wider area; their surveillance is covert and their technological sophistication which means they can capture objects – and, of concern, people – in detail.

Users are urged to be mindful of individual’s privacy during usage of drones given these concerns. The Drones Guidance reminds drone operators that intrusion on privacy can only be justified “if it is proportional to the benefit to...
be derived”, or else it could be considered an unfair collection of data under Hong Kong’s privacy laws.

The non-binding guidance offers four tips for the use of drones: (i) careful planning of a drone’s flight path to avoid flying close to people or properties; (ii) pre-defining recording criteria to avoid over-collection of data and a policy on erasing irrelevant recordings; (iii) ensuring any wireless transmission of data is encrypted; and (iv) providing notice of use of drones by using flashing lights to indicate recording, pre-announcing drone operations, branding the drone to identify drone operators and erecting privacy notices at launch sites.

The guidance also acknowledges certain types of drones may be subject to additional civil aviation regulations or regulation by the Office of the Communications Authority in Hong Kong.

The Drones Guidance also revises the guidance on CCTV previously published in 2010. The guidance has been updated to reflect enhancements in technology and the PCO’s other guidance relevant to CCTV, for example, it expects data users to carry out a privacy impact assessment, warns against use of HD recording, facial recognition and covert surveillance without strong/overriding justification and it specifies that CCTV operators are required to use contractual or other controls to engage third party contractors who provide or maintain CCTV.

Privacy Management Programme – A Best Practice Guide

In January 2014, the Commissioner launched the “Privacy Management Programme – A Best Practice Guide” (“Guide”). The Guide shifts the focus from compliance to accountability as companies are being urged not just to ensure that they comply with mandatory legal obligations but to also manage, handle and be accountable for, customer and employee personal data in accordance with good corporate governance principles.

A Privacy Management Programme (“PMP”) is not a legal requirement under the Personal Data (Privacy) Ordinance (“PDPO”), but the Commissioner advocates that data users should embrace personal data privacy protection at the highest levels of management and apply it as a business imperative throughout the organisation.

The Guide is not legally binding, but failure to comply with the provisions may be taken into account by the Commissioner when investigating whether there has been a breach of the PDPO. As a result, it is important for organisations to be familiar with and embrace the new guidance.

The Guide is divided into 2 parts.

- Part A outlines the baseline fundamentals of a PMP. The key components of a PMP are organisational commitment to a privacy respectful culture (including appointing a data protection officer and establishing an internal reporting mechanism) and programme controls to
ensure compliance with the PDPO (e.g., maintaining a personal data inventory, conducting periodic risk assessments, organising training sessions for employees and devising a data breach handling procedure).

- Part B discusses how to maintain and improve a PMP to ensure ongoing effectiveness, compliance and accountability. For example, the organisation should develop an oversight and review plan to keep the PMP on track and up to date, and periodically monitor its programme controls and revise where necessary.

**Guidance on Cross Border Data Transfer**

In December 2014, the PCO issued the *Guidance on Personal Data Protection in Cross Border Transfer* ("Guidance"). The publication of the guidance has raised many questions about restrictions on cross border data transfer in Hong Kong.

Section 33 of the PDPO was passed into law in 1995 at the time the PDPO was first introduced. However, the section has never been brought into operation. This has not changed. The guidance is voluntary as the Government has not set a firm date for the implementation of Section 33. Nonetheless, organisations are “encouraged” to adopt the practices described in the guidance.

To recap, Section 33 of the PDPO prohibits the transfer of personal data to places outside Hong Kong unless one of the following conditions (“Conditions”) has been met:

1. the destination for the data has been identified by the Commissioner as having laws substantially similar to, or serving the same purpose as, the PDPO (the so-called “White List Jurisdictions”);
2. the data user (sender) reasonably believes that the destination has a law in place that is substantially similar to, or serves the same purposes as, the PDPO;
3. the data subject has given written consent;
4. the data user reasonably believes that the transfer is to avoid or mitigate adverse action against the data subject, that it is not practicable to obtain written consent from the data subject, and such consent would be given if it was practicable;
5. the data falls within one of the exemptions in Part VIII Data Protection Principle 3 (use of personal data) under the PDPO; OR
6. the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data is given equivalent protection to that provided under the PDPO ("Due Diligence Requirement").
The Commissioner has recommended for the Government to have a “renewed focus” on implementing Section 33.

The PCO has stated that it issued the Guidance to assist organisations to prepare for the “eventual implementation” of Section 33 and to provide practical guidance on the expected compliance obligations once Section 33 has been implemented.

The Guidance sets out the Commissioner’s views on practical compliance with Section 33.

**Examples of what is considered to be a transfer:** The Guidance clarifies that transfers of data for the purpose of Section 33 would include:

- the use of a service provider to process personal data outside Hong Kong on behalf of the data user (regardless of the physical location of data storage) - that would include many types of off-shore outsourcing arrangements;
- access to personal data stored in a centralised database in Hong Kong by group companies around the world; and
- access to personal data in a cloud and the cloud server is accessible from outside Hong Kong.

Conversely, the Guidance clarifies that even where data is routed outside of Hong Kong, it is not considered to be a transfer where the sender and recipient of the data are both in Hong Kong.

This is broadly consistent with the approach with respect to transfers in other countries with data protection laws in Asia and in the EU.

**Explanation of the exceptions to Section 33 (the Conditions):** The Guidance explains all six Conditions. Notably:

- for Condition 3 (Written Consent), the example in the Guidance requires that each of the destination jurisdictions be listed in the consent statement and a separate tick box is provided to signify consent to the cross-border transfer; and
- for Condition 6 (Due Diligence Requirement), the Guidance recommends use of the recommended model data transfer clauses included in the Guidance and/or non-contractual means such as auditing and oversight measures.

**The “Recommended Model Clauses”:** The Guidance sets out the recommended model clauses for data transfer agreements but “does not require strict adoption” of these clauses. However, the preamble to Schedule 1 (which contains the model clauses) states that the core clauses are “required” to be included in the data transfer agreement, raising the
question of whether the Commissioner will consider the use of clauses as mandatory once Section 33 has been implemented. We believe that this is the intention.

The core clauses include obligations on both the transferor and transferee, provisions on liability, settlement of disputes and termination. The additional clauses (non-mandatory) include a clause giving third party rights to data subjects under the Contracts (Rights of Third Parties) Ordinance. (The Contracts (Rights of Third Parties) Ordinance was passed into law in December 2014 but is not yet in effect and no effective date has been proposed), and a clause with respect to organisation procedures and data handling.

**Compliance tips for data users:** These include:

- reviewing existing data transfer arrangements;
- limiting unnecessary and unintended data flow;
- checking the White List and understanding how other exemptions apply; and
- maintaining an inventory of data which has been transferred and being transparent about policies and practices.

We consider there are practical issues with the Guidance such as:

- the prescriptive nature of the written consent example - the example requires a list of the jurisdictions to which transfers may be made and a separate tick box relating to the cross border transfer which will be impractical for many organisations.
- the White List has not been published - it is very difficult for organisations to understand the scope of the White List without being able to assess the list itself.
- the present form of the model clauses will present practical and commercial difficulties - for example, the joint liability clause is quite vague in its terms and the termination right enables termination on notice regardless of the materiality of the breach.

As well as stating that compliance with the Guidance is voluntary, the Commissioner has also called for feedback on the value of the Guidance and problems that may be faced in following the Guidance. We believe that submissions from data users in Hong Kong regarding the Guidance will assist in creating a more practical document in future iterations of the Guidance and, at the time of writing, are formulating a response to the Commissioner.
Data Protection Enforcement

In 2014, there were a number of important cases and enforcement actions, including:

- **Mobile Apps**: In December 2014, the Commissioner issued a “Best Practice” guide for mobile app developers. Prior to the release of the guide, a survey of 60 popular mobile apps by the PCO found inadequate transparency in the terms of their privacy policies. In 2014, the Commissioner also found two mobile app developers in contravention of privacy laws - one was excessively collecting personal data and failed to have a privacy policy; the other mobile app developer was in breach for data leakage by the app and failing to take adequate steps to protect the data.

- **Blind Recruitment Advertising**: Employers in Hong Kong need to reveal their identities in job advertisements following the issue of enforcement notices to 48 local employers who had improperly used anonymous “Blind Ads” to collect the personal data of job applicants. The Commissioner said that Blind Ads were an unfair means of collecting personal data and could be exploited as an unscrupulous means to acquire personal data for direct marketing and even for fraudulent purposes.

The Commissioner stressed that employers should refrain from placing Blind Ads for recruitment purposes - the content of advertisements must be carefully considered to avoid unfair collection.

- **Misleading the Commissioner**: A former insurance agent was imprisoned for 4 weeks for making a false statement to the Commissioner during the course of an investigation. This is the first ever conviction under the PDPO for misleading the Commissioner when discharging his statutory functions.

2. Emerging Privacy Issues and Trends

*Bring Your Own Device (“BYOD”)*

The Commissioner updated the *Guidance on Personal Data Erasure and Anonymisation* and *Guidance for Data Users on Collection and Use of Personal Data through the Internet*, to recommend that employers update their policies to include formal “mobile device use” and “BYOD” policies, where employees use their own devices, as well as policies limiting the display of personal data on the Internet by employees.

In addition, data privacy/BYOD is a focus in the banking industry: the Hong Kong Monetary Authority (“HKMA”) issued an updated Circular on Customer Data Protection stating that if banks choose to implement BYOD, they are expected to comply with stringent minimum controls. In October 2014, the
Commissioner also issued the * Guidance on the Proper Handling of Customer’s Personal Data in the Banking Industry* which aims to assist the banking industry to better understand and comply with the relevant requirements under the PDPO in the handling of customer data.

*Social Media: “Privacy Implications for Organisational Use of Social Network” Information Leaflet*

In April 2014, the Commissioner published an information leaflet on “Privacy Implications for Organisational Use of Social Network”.

The information leaflet is not binding but sets out useful examples as to what the Commissioner sees as best practice when organisations use social networks for business purposes.

Key takeaways from the leaflet include:

- aggregated information collected from social networks may identify an individual and therefore will constitute personal data and the PDPO may apply.
- organisations should be transparent with their privacy policies and practices, particularly if data is to be used for marketing or to monitor employees.
- organisations using social networks for recruitment or candidate screening should consider whether the information obtained from the social network is reliable, and can legitimately be taken into account in hiring decisions.

*Do Not Call Registry:*

In August 2014, the Commissioner urged the Hong Kong Government to take steps to combat the increasing prevalence of person-to-person (“P2P”) direct marketing calls by adding them to Hong Kong “Do-not-call” registers. The Government has not taken any further action in response.

3. Law Applicable

The PDPO was enacted on 20 December 1996, and was amended by the Personal Data (Privacy) (Amendment) Ordinance in 2012. The amendments dramatically increased penalties, introduced new offenses particularly focused on direct marketing and unauthorised disclosure of personal data and introduced other changes to strengthen the law.

The PDPO is a principle-based law. Schedule 1 of the PDPO set out the six data protection principles, which govern the collection, use, processing, security, retention/destruction and access to Personal Data. The requirements under the PDPO also apply in the employment context.
The Office of the Privacy Commissioner for Personal Data is the regulatory body that oversees the enforcement of the PDPO. Contraventions of the PDPO may lead to criminal sanctions (fines and/or imprisonment. The maximum penalty for failure to comply with enforcement notice is up to HK$100,000 (approximately US$12,900) and 2 years’ imprisonment. Penalties for direct marketing offenses may be up to HK$1,000,000 (approximately US$129,000) and 5 years’ imprisonment.

Hong Kong also has an anti-spam law, the Unsolicited Electronic Messages Ordinance (“UEMO”), which came into effect on 22 December 2007. The UEMO regulates the sending of unsolicited commercial electronic messages in Hong Kong.

4. Key Privacy Concepts

a. Personal Data
The Ordinance defines “Personal Data” as any data relating directly or indirectly to a living individual and from which it is practicable to ascertain the identity of the individual and which is in a form in which access to or processing of the data is practicable.

“Data”, which the definition of Personal Data encompasses, is defined as any representation of information (including an expression of an opinion) in any document. Personal Data must therefore be in a documented form for it to fall within the scope of the Ordinance.

b. Data Processing
The Ordinance defines “processing” to mean and include amending, augmenting, deleting or rearranging the Personal Data, whether by automated means or otherwise. The Ordinance also has a concept of data “use” which includes the disclosure or transfer of Personal Data.

The Ordinance specifies that data users are liable for the actions of its data processors (e.g., service providers that process data on behalf of a data user). Further, it requires data users to adopt contractual or other means to prevent:

(i) Personal Data transferred to a Data Processor from being kept longer than is necessary for the processing; and

(ii) unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the Data Processor for processing.

c. Processing by Data Controllers
The Ordinance applies to “data users”, that is persons who, either alone or jointly or in common with other persons, control the collection, holding, processing or use of the Personal Data. However, a person is not a data user if he or she holds, processes or uses Personal Data solely on behalf of another person and he or she does not hold, process or use the Personal
Data for any of his or her own purposes. Data processors are not directly regulated in Hong Kong, therefore, the data user is liable for the actions of its data processors.

d. **Jurisdiction/Territoriality**
The Ordinance applies to any collection, holding, processing or use of the Personal Data in Hong Kong. It also applies to all such data users who either have their principal place of business or registered address in Hong Kong.

e. **Sensitive Personal Data**
The Ordinance does not specifically define sensitive Personal Data. All types of Personal Data are subject to the same rules. Note, however, that the PCO issued non-binding guidance in July 2015 on the collection and use of “biometric data”, which it appears to treat as a more sensitive category of data.

f. **Employee Personal Data**
The Code of Practice on Human Resource Management, issued by the Commissioner and effective as of 22 September 2000, applies to employee-related Personal Data. The Commissioner also issued “Privacy Guidelines: Monitoring and Personal Data Privacy at Work” that deals with privacy issues where employees are subject to monitoring. In relation to recruitment, employers cannot seek Personal Data from job applicants, unless there is a position which is or may become vacant.

5. **Consent Requirements**

a. **General**
Except with respect to direct marketing, consent of a Data Subject is not required so long as the data user informs the Data Subject at the time of or before collection of the purpose for which the Personal Data are to be used and the classes of persons to whom the data may be transferred. The Personal Data must be used only for that purpose or a directly related purpose for which it was collected and transferred only to those classes of persons notified as possible transferees on or before collection of the Personal Data. If the Personal Data are to be used in any other way, express consent of the Data Subject is required. A data user is exempted from obtaining such express consent in certain situations prescribed in the Ordinance.

Consent must be given for use of Personal Data for direct marketing or transfer of the Personal Data to a third party for that third party’s direct marketing purpose. Further, if Personal Data is used for direct marketing purposes, the Unsolicited Electronic Messages Ordinance may apply to the sending and the format of commercial electronic messages.
b. Sensitive Data
There are no specific rules that govern Sensitive Data. As such, Sensitive Data is subject to the same consent requirements as other Personal Data.

c. Minors
Consent of minors is not specifically addressed in any laws in Hong Kong.

d. Employee Consent
The general consent requirements also apply in the employment context.

e. Online/Electronic Consent
Electronic consent is permissible and can be effective in Hong Kong if it is properly structured and evidenced.

6. Information/Notice Requirements
Specific requirements apply. A data user must take “all practicable steps” to give the notice on or before the first collection of Personal Data if the data user or its agent collects data from the Data Subject. It is customary to do so in Hong Kong by way of a “Personal Information Collection Statement” or “PICS”.

Data users should include the following information in a Personal Information Collection Statement:

- whether or not it is voluntary or obligatory to provide the data and the consequences of not providing the data;
- the purposes for which the data is collected;
- the categories of persons to whom the data may be transferred;
- that the Data Subject has rights of access and correction; and
- to whom access and correction requests and inquiries in relation to the data user’s data protection policies and procedures should be directed.

Specific information requirements also apply where the data is to be provided for direct marketing purposes. These are detailed in Section 21.

7. Processing Rules
An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfil the identified purpose(s) for which the Personal Data was collected; and delete anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met. (See Section 2 on Excessive Collection of Identity Card Numbers.)
8. Rights of Individuals

Under DPP 6 of the Ordinance, a person whose data is held by a data user is entitled to:

(i) ascertain whether the data user holds data about them; and
(ii) request a copy of and corrections to that data.

The above applies to all Personal Data held by the data user. Exemptions, such as legal professional privilege, apply.

A data user is required to comply with a data access request within 40 days after receiving the request. If it is unable to comply within that time, it must inform the employee in writing that it is unable to do so and give the reasons. Such explanation must be provided before the 40 days expires, and the data user must also fully comply with the request as soon as reasonably practicable after the expiry of the 40 day reply period.

The copy of Personal Data supplied must be such Personal Data as is held at the time when the request is made. Any processing of the data between the time the data access request is received and before the copy is supplied that would have been undertaken irrespective of the receipt of the request is not affected by this requirement. In other words, there is no requirement to stop normal data processing activities because a data access request has been received.

9. Registration/Notification Requirements

Data processors (e.g., service providers that process data on behalf of a data user) are not directly regulated under the PDPO and a data user is fully responsible for the actions of its data processors.

Currently, an organization that collects and processes Personal data is not required to file with the appropriate data authority.

10. Data Protection Officers

In Hong Kong, an organization is not required to designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

Under Section 33 of the Ordinance, the data user cannot transfer Personal Data, except in certain circumstances, including the following:

- the data user has reasonable grounds for believing that the destination jurisdiction has substantially similar provisions to the Ordinance;
- the data subject consents in writing to the transfer; or
the data user has exercised due diligence to ensure that the Personal Data will not be treated in a manner which will contravene the Ordinance.

The above requirements are not yet effective and do not currently form part of the law in Hong Kong. However, in December 2014, the Privacy Commissioner issued voluntary Guidance on Personal Data Protection in Cross Border Transfer (“Guidance”). In the Guidance, the Commissioner has recommended for the Hong Kong Government to have a renewed focus on implementing Section 33. However, no timeline has been set by the Government for implementation of the section. The Guidance sets out the Privacy Commissioner’s views on compliance to prepare for the eventual implementation of Section 33.

12. Security Requirements

DPP 4 of the Ordinance requires that all practical steps be taken by a data user to ensure that personal data it holds is protected against unauthorized or accidental access, processing, erasure, loss or use.

If a data user engages a data processor to process Personal Data on its behalf, the data user must adopt contractual or other means to prevent the unauthorized or accidental access, processing, erasure, loss or use of the transferred data.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

Specific rules apply. For further details on data processing, refer to Section 1 of this chapter and the Commissioner’s information leaflet on Outsourcing the Processing of Personal Data to Data Processors. The Guidance on Personal Data Erasure and Anonymization contains tips on outsourcing to third parties. Industry specific guidance applying to the insurance and finance industries has been issued by the regulators of those sectors.

14. Enforcement and Sanctions

Potential civil and criminal penalties, as well as private rights of action may apply.

15. Data Security Breach


The Breach Guidance Note provides data users with practical steps to be taken in the event that the security of Personal Data is subject to, or is at the risk of, loss, unauthorized or accidental access, processing, erasure or use (“Data Breach”). The Breach Guidance Note confirms that Data Breach
notification is voluntary; however, it suggests that data users should have a Data Breach handling policy in place as a matter of good practice.

In the event of a Data Breach, the Breach Guidance Note sets out four steps to be taken by the data user:

- immediately gather essential information relating to the breach (i.e., when, where and how the breach occurred, what was the cause of the breach and the extent of Personal Data involved);
- adopt appropriate measures to contain the breach (i.e., changing passwords, modifying access rights, and notification of law enforcement agencies);
- assess the risk of harm to the data subject (i.e., risk to personal safety, identify theft, financial loss, risk of humiliation, damage to reputation or loss of business or other opportunity); and
- consider giving a Data Breach notification (particularly where the assessment has shown a risk of personal safety).

In the event of notification, the Breach Guidance Note also provides guidance on who the notification should be given to, what should be included in the notification, when to issue the notification and how to notify the Data Breach.

In the event that the Commissioner is notified, the Breach Guidance Note also provides a Data Breach Notification Form that can be used to give the Commissioner notice of a Data Breach.

16. Accountability

An organization has no legal obligation to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. However, there is a noticeable trend in non-binding guidance recently issued by the PCO to recommend conducting privacy impact assessments before collecting certain sensitive data, such as biometric data, or in circumstances where there is a possibility for excessive collection of personal data, such as when using drones.

17. Whistle-blower hotline

There are no laws/rules that govern whistle-blower hotlines in Hong Kong.

18. E-discovery system

To the extent that the e-discovery system involves the collection, holding, processing or use of Personal Data, privacy issues may arise. The data privacy issues are not, however, confined to e-discovery and will apply in ordinary discovery as well.
19. Anti-spam filter solution

The introduction of a spam-filtering solution is permitted in Hong Kong but would be subject to the guidelines on Monitoring and Personal Data Privacy at Work. Employers should inform employees of their monitoring policy or policies.

20. Cookies

There is no specific law/rule that governs the use and deployment of cookies in Hong Kong.

21. Direct Marketing

*Information and Consent Requirements*

If a data user intends to use, or provide to a third party (i.e., *transfer*), Personal Data for direct marketing purposes, the data user must notify the Data Subject of the following and obtain his/her consent before using the data:

(i) that the data user intends to use or transfer the data for direct marketing purposes;

(ii) that the Data Subject’s consent is required before the data user does so;

(iii) the kind of Personal Data to be used or transferred (e.g., name and email address);

(iv) the classes of marketing subjects to which the direct marketing will relate (e.g., specific categories such as travel and telecommunications); and

(v) in the case of transfer, of the classes of persons to whom the data will be provided (e.g., specific categories such as financial services institutions, telecommunications providers).

(vi) in the case of transfer and if the data is to be provided “for gain”, that the data is to be so provided (“For gain” is defined in the PDPO as the provision of personal data in return “for money or other property” e.g., commissions and fees).

For *use* of data for direct marketing, this information may be provided orally or in writing, and the Data Subject’s consent may be written or oral (although if consent is given orally the data user must send a written confirmation to the data subject within 14 days). For transfer of data, this information must be provided in writing and written consent must be obtained.

The duty to inform the Data Subject of the above information is “absolute” and irrespective of whether the Personal Data is collected from Data Subjects directly or from other sources (e.g., from public registers or third parties).
It is important to note also that if the Personal Data is transferred to a third party for that third party to carry out direct marketing on behalf of the data user, then consent to the transfer is not required.

Transitional Provisions

The new requirements to notify the Data Subject and obtain consent to use of data do not apply if the data user satisfied the following transitional requirements prior to 1 April 2013:

(i) it had explicitly informed a Data Subject that it intended to use the Data Subject’s data for direct marketing for a class of marketing subjects (e.g., specific categories such as travel and telecommunications - generic description is not sufficient);

(ii) it had been using the Personal Data for that purpose;

(iii) it had not been requested by the Data Subject to cease using the data for that purpose; and

(iv) it had not otherwise contravened the PDPO in relation to that use.

The transitional provisions apply only to use of data, not to provision of data to a third party, for direct marketing purposes. Therefore, from 1 April 2013 consent will be required for providing (i.e., transferring) Personal Data to third parties for direct marketing.

First Use of Data

A data user is required, when using Personal Data for direct marketing purposes for the first time, to notify the Data Subject that the data user is obliged to cease using their Personal Data on request and provide a means for the Data Subject to object. If the Data Subject, at any time after collection of their Personal Data, requests that a data user stop using or transferring its Personal Data for marketing purposes, then the data user must cease such activities. The maximum penalty for violations of this requirement have been increased from HK$10,000 (approximately US$1,290) to HK$500,000 (approximately US$64,000) and up to 3 years’ imprisonment.

Penalties

Non-compliance with any of the information or consent requirements, using Personal Data without consent, or failing to cease use after an objection has been received, all carry penalties. The penalties for offenses with respect to use of Personal Data for direct marketing is punishable by a fine of up to HK$500,000 (approximately US$64,000) and 3 years’ imprisonment. The penalties for offenses with respect to provision of Personal Data for direct marketing are also punishable by a fine of up to HK$500,000 (approximately US$64,000) and 3 years’ imprisonment, however if the transfer is for gain (i.e., payment), the maximum fine is HK$1 million (approximately
US$129,000) and 5 years’ imprisonment. It is a defense for the data user to show that it took all reasonable precautions and exercised all due diligence to avoid commission of the offense.

**Guidance on Direct Marketing**

On 15 January 2013, the Commissioner published the New Guidance on Direct Marketing ("**New Guidance**"), which provides some practical guidance on compliance with the new direct marketing regime.

**Consent**

Under the PDPO, “consent” is defined to include “an indication of no objection”. The New Guidance provides that there must be “explicit” action taken on the part of the Data Subject to qualify as “an indication of no objection”. In other words, silence will not constitute consent. For example, consent can be in the form of an opt-in (e.g., by asking a customer to check a tick box when signing a form) or an opt-out (e.g., by providing a customer with the opportunity to opt-out of receiving marketing and confirming that he/she agrees to the use of data in direct marketing). An opt-out is only valid where an active step is taken by the Data Subject to submit their data such as signing a form or clicking “I accept”.

The “opt-out later” or “deemed consent” approach that was acceptable in the past is no longer sufficient. For example, where a company informs a customer in writing of the use or provision of Personal Data for direct marketing and states that “any objection has to be made by sending back the objection slip”, such a non-response from the Data Subject would not amount to valid consent.

The New Guidance also provides that “**bundled consent**” should be avoided. **Bundled consent** is where direct marketing consent language is inseparable from other provisions in an application form or contract terms and there is no option for the customer to object to the direct marketing use and still obtain the other services applied for. Data users should not design application forms and contracts in a way which makes it impracticable for a customer to refuse the use of their personal data for direct marketing purposes (for example, by providing only one space to sign on an application form for a product/service).

**Classes of Marketing Subjects**

The examples provided in the New Guidance suggest that the description must be very specific. Companies should make reference to the distinctive features of the goods, facilities or services so that customers may ascertain the types of goods, facilities or services about which they may receive direct marketing with a “reasonable degree of certainty”. For example, “telecommunications network services offered by ABC Company” would be acceptable, but “retail services and products provided by ABC Company” would not be acceptable as it is too broad for customers to comprehend the
actual classes of goods, facilities or services. The information must be provided in an easily readable and easily understandable manner.

*Individuals in a Business Capacity*

The New Guidance draws a distinction between marketing targeted at individuals or their employing corporations. This is significant as it goes beyond the strict interpretation of the Amendments. Where Personal Data is collected from individuals in their “*official capacity*” (for example, as in-house legal counsel) and the product or service is clearly meant for the exclusive use of the corporation by whom the individual is employed, the Commissioner takes the view that the requirements of the new direct marketing regime *will not* apply. However, if that same individual is sent details of products or services targeted to them as an individual, the direct marketing requirements *will* apply.

*Transfer to Affiliates*

The New Guidance clarifies that it is a misconception that a data user may freely transfer Personal Data to its parent company and subsidiaries/associated companies for direct marketing purposes. Now that the new direct marketing regime is in effect, a data user is required to obtain written consent from a Data Subject prior to providing personal data to any other person or entity for the purposes of direct marketing, including affiliates. There are no transitional provisions applicable to transfer of data for a third party’s direct marketing purposes.
Hungary

Adam Liber
Budapest
Tel: +36 1 302 3330
adam.liber@bakermckenzie.com

Ines Radmilovic
Budapest
Tel: +36 1 302 3330
ines.radmilovic@bakermckenzie.com
1. Recent Privacy Developments

Authorization of BCRs and Data Breaches Registry


The Amendment provides that the Hungarian National Authority for Data Protection and Freedom of Information (“Authority”) may approve the implementation of Binding Corporate Rules (“BCRs”) as an adequacy instrument for data transfers from 1 October 2015. (Previously, the Hungarian data protection laws previously omitted BCRs from the list of recognized “adequacy” instruments). The Amendment contains no transitional provisions regarding BCRs already approved by the data protection authority of another EU Member State, however. It is therefore currently unclear - and further guidance from the Authority will be needed concerning - how the Authority will treat such BCRs. Depending on the Authority’s future guidance, companies whose EU BCR cooperation procedure is already closed might be required to make a formal filing with the Authority to enable the use of BCRs in Hungary.

The Amendment also contains provisions regarding the treatment of data breaches by Data Controllers under Hungarian data protection laws. Data breach notification will continue to apply only with regard to telecom providers. However, the Amendment will impose an obligation on Data Controllers to keep a register of data breaches, including any measures introduced by the Data Controller to remedy such breaches. This new provision only applies to Data Controllers. But existing data processing agreements will need to be amended because Data Processors will also be required to register data breaches on behalf of the Data Controller. Thus, the processing agreement should contain detailed provisions regulating how the Data Processor should comply with such obligations relating to the recordal of data breaches.

Finally, the Amendment will introduce higher fines; the Authority will be able to impose a data protection fine of up to HUF 20 Million – twice the current maximum fine amount of HUF 10 Million.

The Amendments enter into force on 1 October 2015.

Single registration of data processing for marketing promotions organized at different times

In 2014, the Authority issued an opinion confirming that data processing activities relative to marketing promotions organized at different times by the same Data Controller may be registered with the Authority through one single registration, provided that the circumstances of the various data processings (i.e., the purpose of data processing, the legal basis of data processing, scope of data subjects, categories of personal data to be processed, the source of
the data, the duration of processing, the categories of data transferred, the recipients and the grounds for data transfers) are the same with respect to each of the different promotions. According to the Authority, in such cases, the Data Controller should notify the Authority, for example in an e-mail sent together with the initial data processing registration request, that the registration covers various future data processing activities; then, no notification to the Authority will be required in the subsequent cases.

**Recommendation on privacy requirements applicable to the various techniques used in the course of claim enforcement, debt recovery and factoring**

The Authority issued a recommendation on the privacy requirements in respect of various techniques used in claim enforcement, debt recovery and factoring, on the basis of several cases in which the Authority established the infringement of the Data Protection Act by entities engaged in those activities. The recommendation distinguishes between businesses engaging in those activities based on (i) the assignment of the underlying creditor’s claim, or (ii) a mandate from the creditor. The Authority stated that, in the first case, credit management companies may process the personal data of debtors purely on the basis of the assignment because, as a matter of Hungarian civil law, that assignment does not require the consent of the debtor and so personal data automatically transfers with the assignment. On the other hand, in case debt recovery is conducted upon a mandate from the creditor, the legal grounds of the processing the debtors’ personal data may be either (i) the consent of the debtor, (ii) the specific authorization of a law or (iii) the debt recovery activity conducted by an attorney-at-law. The Authority also emphasized the importance of the Data Subject receiving proper advance notification about whether or not his/her consent is required for data processing relative to the debt claim enforcement. Also, the Authority gave a detailed recommendation about the requirement of necessity, proportionality and fairness of the data processing relative to the use of drones and concluded that, among others, the collection or processing during such activities of third persons’ (relatives, neighbors) personal data is excluded.

**Recommendation on the use of drones**

The Authority issued an extensive recommendation on the use of drones for business and private purposes and also organized a conference on this subject. The Authority stated in its recommendation that, whereas the use of drones by the state or by business for commercial purpose falls within the Data Protection Act, the use of drones by individuals for private purposes is currently excluded from the scope thereof. The recommendation deals, among others, with the purpose, scope, legal basis, necessity, proportionality, data security of the data processing relative to the use of drones as well as with the obligation to provide information. In its recommendation, the Authority
urged the Hungarian legislators to adopt a specific law regulating the use of drones and containing provisions on data protection issues.

2. Emerging Privacy Issues and Trends

*Practice of the Authority*

While the Authority continues to interpret the Data Protection Act in a conservative manner, in some instances, the Authority is becoming more business friendly, and consequently, it has shown a willingness to accept reasonable business arguments raised by Data Controllers. The Authority places an emphasis on the enforcement of the restrictive Data Protection Act as prescribed by the Data Protection Directive and as interpreted by the Article 29 Data Protection Working Party.

The Authority is entitled to impose sanctions for the violation of the Hungarian data protection rules. In the past years, the Authority examined the lawfulness of data processing in connection with, among others, manpower-leasing, online dating services, real estate agency services, organization of promotions, and claim enforcement. In 2014, the Authority focused on claim enforcements and debt-recovery services, the organization of product presentation events and on online direct marketing services. The Authority publishes most of its resolutions on its website.

In 2014, the Authority initiated 30 administrative proceedings and imposed fines of HUF 78 million in the aggregate. In 2015, the enforcement priorities of the Authority are investigations relating to the data processing activities of debt collection agencies, data processing for product presentation events (“roadshows”), as well as data processing for telemarketing purposes.

*Cooperation between Hungarian authorities*

In the spring of 2014, the Authority concluded cooperation agreements with the Hungarian Competition Office and the Hungarian National Bank in order to help each other’s activities and to cooperate in issues regulated by the Data Protection Act. In that framework, the Authority will assist the two other authorities in interpreting the privacy related questions they encounter.

*Request for a preliminary ruling from the CJEU – Weltimmo s.r.o. v the Authority (Case C-230/14)*

The highest court of Hungary requested a preliminary ruling from the CJEU in the so-called Weltimmo case which was initiated by the Authority relative to the infringement of the Data Protection Act by a Slovakian company operating a website advertising Hungarian properties for sale. One of the court’s questions submitted to the CJEU is: ‘whether Article 28(1) of the Data Protection Directive could be interpreted in a way that the provisions of national law of a Member State are applicable in its territory to a situation in which a data controller runs a property-dealing website established only in
another Member State and also advertises properties situated in the territory of that first Member State and the property owners have forwarded their personal data to a facility (server) for data storage and data processing belonging to the operator of the website in that other Member State’. The CJEU is currently reviewing the case; it is unclear when the CJEU’s ruling will be delivered. The Advocate General’s opinion on this case was published on 25 June 2015.

**Authority’s Guidance impacting M&A transactions involving web shop assets**

The Authority recently released guidance on issues arising in the context of the sale of the assets of an online shop. This is the Authority’s first guidance on the practical application of the “legitimate interest” test under Hungarian data protection laws and is relevant to M&A transactions involving online shops.

The sale of the assets of an online shop involves situations where domains, goods, trademarks and client databases as a whole are sold by one online shop operator to another, without the purchase/transfer of shares. The transfer of client databases (including Personal Data) is ancillary that asset sale transaction. The Authority has taken the position that the transfer of the client database in such a transaction constitutes a Personal Data transfer under the Data Protection Act and must be legitimized by an appropriate legal basis for the data processing. However, the Authority underlined that the parties to the transaction do not necessarily need to rely upon the freely given, express advance consent of the Data Subject provided that such transfer may be justified by other legal reasons - such as by the legitimate interest clause contained in the Data Protection Act or in Article 7(f) of the EU Directive (which is directly effective in Hungary) (see joined cases C-468/10. and C-469/10. of the CJEU).

The Authority described the “legitimate interest” (or balance of interests) test as having three prongs: (i) the identification of the legitimate interest of the Data Controller; (ii) the identification of the legitimate interest or fundamental right of the Data Subject; and (iii) the requirement that those two weights be balanced against each other in order to determine if the “legitimate interest” may be relied on as the legal basis for data processing in the given situation. In that context, the Authority suggested considering the following key factors when applying the test:

- The seller must provide clear and comprehensive information to the Data Subjects (i.e., the online shop’s customers) on the outcome of the test performed by the seller, explaining why it considers that its interests outweigh the restriction on the interests and rights of the Data Subjects. The seller’s notice to the Data Subjects must include the details of the transfer, such as its date, the identity of the recipient of data, and the main details of the asset sale transaction;
• Before the data is transferred to the new online shop operator, the seller (i.e., the Data Controller) must provide to the Data Subjects the effective possibility to object to the transfer of their Personal Data to the buyer;

• The buyer must remain bound by the conditions under which the seller processed the Personal Data of the Data Subjects. The data processing conditions may not change as a result of the data transfer to the new Data Controller. However, this does not impact the right of the new Data Controller to engage a new Data Processor (which, in any case, does not require the data subject’s consent).

The Authority also noted that certain processing activities (such as the retention of invoices) are based on the provisions of the accounting laws. If the seller and the buyer have agreed that the seller will retain the accounting documents, said data transfer is considered to be based on a legal provision. However, the Authority underlined that the notice to the Data Subjects also must include information about transfers of Personal Data the processing of which is based on a legal provision.

3. Law Applicable


*Act No. I of 2012 on the Labor Code (“Labor Code”), which applies to employee related data processing

*Act C of 2003 on Electronic Communications (“Electronic Communications Act”)

*Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators

*Act CVIII of 2001 on Electronic Commerce and on Information Society Services (“E-Commerce Act”)


*Act No. CXIX of 1995 on the Handling of Names and Addresses for the Purposes of Scientific Research and Direct Marketing

*Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities

*Act No. XLVII of 1997 on the Protection of Personal Data Regarding Healthcare and Related Issues (“Healthcare Data Protection Act”)

*Act No. XXXV of 2001 on Electronic Signatures (“Electronic Signature Act”)

*Act No. CLXV of 2013 on Complaints and Public Interest Disclosure (“Whistleblowing Act”)
Further, sector-specific legislation, such as banking laws, social security laws, tax laws etc., contain additional data protection rules, particularly relating to the legality of data processing and the data retention obligation of Data Controllers.

Although the recommendations of the previous Data Commissioners and those of the new Authority do not qualify as law, they are generally followed in practice. Further, the Authority tends to consider and follow the recommendations of the Article 29 Data Protection Working Party, established under the Data Protection Directive.

4. Key Privacy Concepts

a. Personal Data

The Data Protection Act applies to the processing of any information relating to or otherwise connected to an identified or identifiable natural person (“Data Subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, or social identity. Any conclusion concerning the natural person that can be drawn from the processed information also qualifies as protected Personal Data (“Personal Data”). In the course of data processing, such information is treated as Personal Data as long as the Data Subject remains identifiable. Thus, the term Personal Data is widely defined.

b. Data Processing

The Data Protection Act defines data processing similar to the way it has been defined under the Data Protection Directive. However, the Data Protection Act uses the term “data controlling” for that activity. The term “data processing” means limited, rather technical data processing activities performed by Data Processors, as described below. For the purpose of this summary, we use the term, “Data Processing” within the meaning of the Data Protection Directive.

“Data Processing” is widely defined and includes collecting, recording and storing, processing, utilizing (including forwarding and publishing), data altering, and preventing further use of the Personal Data. Photographing, sound and video recording and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples, and retinal images) would also qualify as processing. The Data Protection Act applies to manual, partially automated and automated Data Processing.

c. Processing by Data Controllers

The Data Protection Act applies to those persons, including any natural or legal person or organization which alone or jointly with others determines the purpose for which and the manner (including the means used) in which any Personal Data is or will be processed and who execute the Data Processing, or who appoints someone to process Personal Data (“Data Controller”). A
Data Controller is responsible for the Data Processing, including for the activities of its Data Processors. When deciding whether a person qualifies as a Data Controller or a Data Processor, the Authority tends to classify a person who has even a minor decision-making right in respect of Data Processing as a Data Controller and not as a Data Processor.

The Data Protection Act also applies to “Data Processors”. According to the Data Protection Act, a Data Processor performs technical data processing activities at the instruction of the Data Controller. Processing by a Data Processor is defined by the Data Protection Act as the performance of technical tasks related to Data Processing operations, regardless of the methods or means used or of the place of the location of the application. Data Processors are not entitled to make decisions on the merits of data processing (e.g., may not decide to forward Personal Data to a third party, unless instructed by the Data Controller). The Data Processor may subcontract its data processing activities and employ further Data Processors with the consent of the Data Controller.

d. Jurisdiction/Territoriality

The Data Protection Act applies to the processing of Personal Data (including automatic or manual data processing) on the territory of Hungary, unless the Data Processing is carried out solely for the Data Subject’s own (household) purposes (such that said Act does not apply to the private data processing activities of individuals). Furthermore, the provisions of the Data Protection Act are applicable if a foreign Data Controller (processing Personal Data outside the EU) employs a Data Processor whose registered address or place of business (branch) or habitual residence is situated in Hungary or if it makes use of equipment situated in Hungary, unless such equipment is used solely for the purpose of data traffic exclusively within the territory of the European Union. In such a case, the Data Controller must appoint a representative in Hungary. If Personal Data is transferred outside Hungary, the general rule is that the Data Protection Act applies to data transfer.

The territorial scope of the E-Commerce Act which also contains some data protection rules is broader than the territorial scope of the Data Protection Act. This legislation may be relevant when a service provider situated outside the European Union directs e-commerce and/or information society services to Hungary.

e. Sensitive Personal Data

The Data Protection Act imposes additional requirements relating to the processing of “Sensitive Personal Data” – that is, Personal Data relating to racial, national, or ethnic origin, political opinions or political party membership, religious or other convictions, membership in a society, association or trade union, health condition, abnormal addiction, sexual orientation, and criminal records.
Sensitive Personal Data may be processed only if:

- the Data Subject gives his/her written consent to the Data Processing;
- the Data Processing is required under an international convention or by an Act of Parliament for the purpose of enforcing a fundamental constitutional right, or for national security purposes, crime prevention, or criminal investigation;
- the Data Processing is otherwise required by an Act of Parliament in the interest of the general public – e.g., it is performed by a health care professional for such purposes which are defined by law; or
- the Data Processing is otherwise authorized based on Section 6 of the Data Processing Act.

f. Employee Personal Data

The Labor Code contains only a few general rules on employment-related Data Processing. In the absence of specific rules, in case of employment-related Data Processing, in addition to the Labor Code, the Data Protection Act must also be applied.

Under the Labor Code, an employee (or job applicant) may be requested to make a statement or to disclose information only if it does not violate his/her personal rights and which is deemed necessary for the conclusion, maintenance or termination of the employment relationship. The opportunity to require an employee (or job applicant) to take an aptitude test, provide background information or to perform a detailed background check is limited.

An employer has a general obligation to inform its employees concerning the processing of their Personal Data. Although an employer may monitor employees in connection with the performance of their obligations, the employer must notify its employees concerning the means and methods the employer uses for this purpose. The private life of employees may not be monitored or violated in any manner.

The data protection and personal rights of employees may be restricted if deemed strictly necessary for reasons directly related to the intended purpose of the employment relationship and if proportionate for achieving its objective. The means and conditions for any restriction of personal rights and their expected duration must be communicated to the employees in advance.

---

1 For example, the new Labor Code provides an opportunity to check/control employee’s work during working time. However, the Labor Code contains only some general rules and does not provide a detailed description on how and to what extent employers may exercise their control rights. As exercising the control rights affects the data protection rights of the employees and in certain cases, also the rights of third parties, the Data Protection Act has to be considered as well and applied together with the Labor Code.
Data Processing by the employer may be conducted if it is (i) authorized or
(ii) required by law. The statutory authorization to process Personal Data of an
employee (including Sensitive Personal Data), however, covers only the
minimum Data Processing activities which are strictly required to perform the emplement relationship and to comply with statutory obligations.

Also, the Authority – based on its published guidelines – is of the view that the consent of the employees may only serve as legal grounds for Data Processing in cases where the voluntary nature of the employee’s consent may clearly be ensured. In line with this, the Authority also stated that an employer – in certain cases – may rely on its legitimate interests as the legal grounds for the Data Processing only if enforcing such interest is considered proportionate to the limitation of its employee’s right to the protection of Personal Data.

As the Labor Code contains only a few rules on this issue, employers must prepare a privacy policy, in which the most important rules, such as those on the usage of company equipment, the controlling rights of the employer etc. are stated. The employer, by the adoption and distribution of an adequate privacy policy, can simultaneously ensure compliance with its statutory information obligation and ensure that it is entitled to exercise its monitoring rights as described in the policy.

5. Consent

a. General

Consent of the Data Subject is one of the legal ground for processing Personal Data in Hungary based on the informational self-determination right of the data subject.

The Data Protection Act provides for exemptions to the consent requirement in cases where the processing of Personal Data is necessary for the purposes of the legitimate interest pursued by the Data Controller or by a third party and enforcing those interests is considered proportionate to the limitation of the right to the protection of Personal Data or where processing is for compliance with a legal obligation. Consent by the Data Subject must always be voluntary, informed (i.e., based on accurate and detailed information), explicit and unambiguous. To be unambiguous, the consent must be a clear indication of the Data Subject’s agreement to the processing of Personal Data relating to him, without limitation or with reference to specific operations, though consent is not required in certain prescribed circumstances.

Consent may be express or implied; the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and the sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to cover only the identified purpose(s). A new consent is required for purposes which were not previously identified and consented to.
There is no requirement that consent must be in writing. It may be provided orally or in other forms/formats. In addition, the Data Subject also has the right to withdraw consent at any time in given circumstances.

b. Sensitive Data
Where consent is relied upon to justify the processing of Sensitive Personal Data, it must have been obtained in writing prior to the processing.

c. Minors
Under general Hungarian law rules, a person under the age of 18 is usually considered a minor, who may make valid legal declarations (e.g., conclude contracts) if the minor’s legal representative (i.e., parent, guardian, etc.) consents to those declarations. Minors between the ages of 14 - 18 have limited legal capacity to conclude certain contracts. The Data Protection Act contains a special rule applicable to minors over 16. Under that rule, the consent of such a minor is valid without the consent or subsequent approval of the minor’s legal representative.

d. Employee Consent
The Labor Code states that the employer may disclose Personal Data to a third party only in the cases specified by an Act of Parliament or with the employee’s consent. In that context, a related company of the employer or another member of the group of companies of which the employer is a member of also qualifies as a third party. The Labor Code does not require that the consent be given in written form.

However, in its guidance, the Authority stated that the employee’s consent may serve as the legal grounds for Data Processing only in cases where the voluntary nature of the employee’s consent may clearly be ensured. This guidance indicates that employers should rely on other legal grounds when processing their employees’ Personal Data, e.g., statutory authorization and/or the legitimate interests pursued by the employer as Data Controller provided that enforcing these interests is considered proportionate to the limitation of the employee’s right to protection of Personal Data.

e. Online/Electronic Consent
In cases where the Data Protection Act requires written consent, the consent may be given in an electronic document signed by an advanced electronic signature (in this case, an electronic consent qualifies as a written consent). Electronic signatures, however, are not widely applied in Hungary. According to the practice of the Authority, pre-checked boxes may not be used to signify the affirmative consent of the Data Subject.
6. Notice Requirements

An organization that collects Personal Data must provide clear and detailed information to Data Subjects about all relevant aspects of data processing, including; the organization’s identity; the types of Personal Data being collected; the legal bases and purposes for collecting Personal Data; the organization’s privacy practices (which must be given in a clear and transparent way); the identity of the third parties to which the organization will disclose the Personal Data; the rights of and the legal remedies available to the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; and how to contact the privacy officer or other person who is accountable for the organization’s policies and practices. The Data Controller must inform the Data Subject if the Data Controller relies on the legitimate interest test as a legal basis of data processing. If the provision to the Data Subject of such notice proves impossible or would involve disproportionate costs to the Data Controller, the notice may be published in a way which makes it publicly accessible to the Data Subjects.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion, blocking and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

The general rule is that every data processing activity has to be notified to the Authority but the Data Processing may not be commenced before the earlier of the receipt of the Authority’s confirmation of said notification or the 9th day following the submission of such notification, provided that the notification contains all the relevant information required by law. (Implied authorization) There are several, strictly interpreted exemptions, however, which include Data Processing for the purposes of maintaining an employment, customer (but excluding communications service providers, banks or insurance companies) or supplier relationship.
10. Data Protection Officers
The appointment of a data protection officer is required by law only in the case of financial institutions, public utility companies and telecom companies.

11. International Data Transfers
Notwithstanding the medium or the manner of the data transfer, Personal Data (including Sensitive Personal Data) may be forwarded outside Hungary to non-EU countries only if:

- the Data Subject gives his/her explicit consent; or
- the conditions of the Data Protection Act are met and the laws of the non-EEA third country in question afford an adequate level of protection.

An adequate level of protection is achieved:

- if the European Commission, in its decision, determines that the third country in question ensures an adequate level of protection (such as Safe Harbor);
- if the transfer is prescribed by a bilateral treaty containing guarantees for the rights of Data Subjects, their rights to remedies, and for the independent control of processing;
- even if the above rules are not complied with, to enforce the provisions of an international legal aid treaty (such as MLATs) or of a treaty on the avoidance of double taxation, under the terms of those treaties;
- an adequate level of data protection may be ensured by the use of EU model clauses; or
- from 1 October 2015, through the use of BCRs subject to the approval of the Authority.

The Data Protection Act does not allow the transfer of Personal Data to third countries where adequate protection is ensured through *ad hoc* contractual clauses. In practice, data controllers rely on adequacy decisions or use the relevant EU model clauses, adopted by the European Commission, for international data transfers.

If there are no laws authorizing the transfer, the consent of the Data Subject will be required. Transfer of data to EEA member states is treated as a transfer within Hungary if Personal Data is transferred in order to process it.

12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in its possession and control is protected from unauthorized access and use; implement appropriate physical, technical and organization security
safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved. The Data Protection Act requires additional security measures to be introduced in relation to the automatic data processing activities. This must cover measures securing:

- the prevention of unauthorized input of data;
- the restriction of use of data transfer devices by unauthorized persons;
- the control and recording of data transfers to organizations that are or may be made by data transfer devices;
- the monitoring and supervision of the input of personal data into automated data processing systems by recording the identity of the person who made such input and the time when such input was made;
- the recovery of the systems in case of any malfunction; and
- the maintenance of a log file and a report of malfunctions or failures.

13. Special Rules for Outsourcing of Data Processing to Third Parties

In 2013, the Authority examined international data transfer requirements and indicated that if data is transferred to a third country based on the Data Subject’s explicit consent, the Data Subject must clearly state that he/she has understood the possible risks arising from the data transfer and agrees to such transfer of his/her Personal Data. Accordingly, prior to obtaining his/her consent to such data transfer, the Data Controller must inform the Data Subject that his/her Personal Data could be transferred to third countries which do not provide the necessary level of protection of Personal Data.

Regarding the transfer of employees’ Personal Data to third countries, the Authority stated that the consent of the employees may serve as the legal grounds for data processing only if the voluntary nature of the employee’s consent may clearly be ensured. The Authority also stated that an employer is expected not to transfer its employees’ Personal Data to countries without adequate levels of data protection.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, authority investigations/audits, authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.
15. Data Security Breach

There is no obligation under Hungarian laws for organizations that are involved in a data breach situations to inform the Data Subjects or authorities about the breach except for a specific regime applicable only to electronic communications services providers as regulated in the Electronic Communications Act. The organization may be required to gather information about the breach, assess the potential risk of harm to the Data Subjects, take steps to prevent future similar breaches and assist authorities with any investigation relating to the breach.

If, during a data protection audit, a security breach is discovered by the Authority, the Data Controller could be subject to various sanctions for non-compliance with the processing rules. If the Data Subject discovers such a breach, he or she may claim damages as a result of the breach.

An organization that is involved in a data breach situation may be subject to suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, or civil actions and/or class actions.

As of 1 October 2015, Data Controllers must keep a register of data breaches, including any measures introduced by the Data Controller to remedy such breaches. This new provision applies only to Data Controllers. But existing data processing agreements will need to be amended because Data Processors also will be required to register data breaches on behalf of the Data Controller. Thus, the processing agreement should contain detailed provisions regulating how the Data Processor should comply with such obligations relating to the recordal of data breaches.

16. Accountability

Subject to regulatory guidance, organizations may be obliged to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. Organizations may also be required to furnish to privacy regulators evidence relating to the effectiveness of the organization's privacy management program.

17. Whistle-blower hotline

Under the Whistleblowing Act, an employer and its owner(s) are authorized by law to establish a whistleblowing system, should they wish to operate one, to investigate reports about violation of laws or rules of conduct issued by the employer, provided that such rules of conduct protect a public interest or a significant private interest. In order to investigate whistleblowing reports, the employer may process and transfer to third parties participating in the investigation the Personal Data indicated in the report of the reporter and of the person(s) to whom the report refers. Reporting persons may include
employees, contractors or any third person having a legitimate interest in making the report or in remedying the reported situation.

The Whistleblowing Act requires that the data processing related to the whistleblowing system must be notified to the Authority. In addition, the employer must disclose on its corporate website the rules of conduct of the whistleblowing system, as well as a detailed description of the reporting procedure, in Hungarian.

The Whistleblowing Act permits data to be transferred abroad only if adequate protection of the transferred data is ensured and the foreign Data Controller and Data Processor make a contractual commitment to comply with the provisions of the Whistleblowing Act.

18. E-discovery
The implementation of an e-discovery system without the informed consent of the Data Subject raises serious data protection and privacy issues. Even if the Data Subject has granted consent, certain discovery measures may still be considered infringing (e.g., monitoring of private e-mails).

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented. Though not mandatory, employers may give employees the opportunity to opt-out from the spam-filtering solution and the opportunity to review the isolated emails designated as spam.

20. Cookies
There are no specific laws/rules that regulate the deployment of cookies except for those applicable only to electronic communications service providers and laid down in the Electronic Communications Act, and hence, the use of cookies must comply with data privacy laws. In general, consent of Data Subjects must be obtained before cookies may be used. Some types of cookies that track or monitor the user may not be permitted under Hungarian law.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond to the request for his/her consent. An organization must obtain consent for a specific marketing activity. Bundled consent is not considered valid consent.
Iceland

Hjördis Halldórsdóttir
Reykjavik
Tel: + 354 5 400 300
hjordis@logos.is
1. Recent Privacy Developments


The Data Protection Act provides for the establishment of a specific institution, the Data Protection Authority (the “DPA”), which is responsible for monitoring the application of the Act and the administrative rules that are based on it.

The DPA registers more than 1,200 matters each year. The most notable rulings in the recent years are the following:

• On 25 February 2015, the DPA ruled in two cases regarding a “fraud button” on the Social Insurance Administration’s webpage. In both cases, No 2014/832 and No 2014/1068, the DPA held that as the notifications could be sent anonymously, the data subject’s right e.g. to know where the information came from could not be secured. All collection and processing of such personal data were held to be in breach of the Data Protection Act.

• In a ruling by the DPA, dated 9 February 2015 in case No 2014/884, a former employee complained to the DPA as his former employer had not closed his e-mail account and e-mails from his account were forwarded to the company’s general e-mail address. The DPA found that this was contrary to rules No 837/2006 on electronic surveillance, as the employer could not prove that the employee had specifically provided his consent for the transfer.

• On 14 December 2014, the DPA issued a ruling in case No 2014/796 where a complaint was submitted to it on the collection of biomedical samples by Decode. The complainant was of the opinion that the way in which these samples were collected was in breach of the Data Protection Act. However, as the collection of samples was not done for the purpose of marketing, business or profits, but for the sole purpose of improving health and curing diseases, the DPA found that Decode was allowed to collect these samples by knocking on peoples’ doors and by disregarding public ban lists for marketing. The DPA also found that the processing of the data did not go against the Act as it was based on the clear consent of participants.

• On 22 October 2014, the DPA gave an opinion, No 2014/1134, on whether or not landlords were allowed to seek personal data on tenants before signing tenancy agreements. The DPA found that landlords were entitled to seek information on (a) the general identity of tenants, such as confirmation of employment, pay slips, registered defaults, copies of
passports and marital status and (b) sensitive personal information such as criminal records. Landlords would however have to make sure that all processing would comply with the requirements of the Act and be carried out with proportionality and fairness.

- On 25 January 2012, the DPA passed a ruling in case No 2012/531 where it found that any personal data that has been collected through a “fraud button” on an insurance company’s webpage, where notification on insurance frauds can be sent anonymously, shall be deleted as soon as the data subject requests deletion.

- On 12 October 2011, the DPA passed a ruling in case No 2011/84 where it found that CCP, an online video game company, contravened the Act by transferring a player’s personal data to the USA and China. The DPA found that a data subject who accepts a company’s privacy policy, which refers to transfer of personal data to third countries without specifying which countries, is not considered to have accepted a transfer of his/her personal data to countries that do not provide an adequate level of personal data protection.

In recent years, no significant amendments have been made to the Data Protection Act. In 2014, two minor amendments were however made stating that (i) health science research is now subject to specific permission in accordance with the Act on Scientific Research in the Biomedical Field No 44/2014 and (ii) information that falls under the scope of the Data Protection Act may be handed to a Public Archive for preservation according to the Act on Public Archives No 77/2014.

2. Emerging Privacy Issues and Trends

- **Mandatory Breach Notification**: There is no mandatory requirement in the Data Protection Act to report data security breaches or losses to the DPA. However, a notice is considered as good practice, particularly if the security breach is major.

- **Direct Marketing**: Based on Article 46 of the Icelandic Electronic Communications Act No 81/2003 (the “ECA”), the use of automated calling systems, facsimile machines or electronic mail for direct marketing is only allowed if a subscriber has given prior consent. Electronic mail addresses obtained in the context of the sale of a product or service may however be used for direct marketing of own goods or services if customers are given the opportunity to object to such use of addresses free of charge when they are listed and similarly each time a message is sent, if the customer has not initially refused such use. Users who use public telephone services as part of their marketing must respect designations in a telephone directory indicating that the subscriber in question does not wish to receive such calls to his/her number (Do Not Call Registry).
• **Cloud computing and social media**: No specific legislation has been passed, however all processing must comply with the Data Processing Act. In relation to cloud computing, the question on where the data is stored has lead the DPA to conclude that a processor cannot, in all events, be considered to fulfill the Act’s requirements concerning security measures.

• **Electronic Signatures**: The Act on Electronic Signatures No 28/2001, which implemented Directive 1999/93/EC of the European Parliament and of the Council on a Community Framework for Electronic Signatures, stipulates that fully qualified electronic signatures shall have the same effect as handwritten signatures. Furthermore, it is stipulated that other electronic signatures can be legally binding. Icelandic legislation faithfully follows the definitions of the European Directive.

• **Binding Corporate Rules**: International companies are allowed to transfer personal data between operating bases, across borders, if the company has applied the so-called Binding Corporate Rules. Such rules are intended to ensure that within each company falling under their scope, all personal data is given adequate protection. Their binding value is based on the companies’ unilateral commitment to the rules. However, for the transfer of data across borders to be lawful under the Binding Corporate Rules, it must have been authorized by the DPA.

• **Data Protection Enforcement**: The Data Protection Authority has the power to impose daily fines until it concludes that the necessary improvements have been made. If the Authority’s decision to impose daily fines is referred to the courts, then the fines will not begin to accrue until a final judgment has been rendered. The Authority can assign to the Chief of Police the task of temporarily halting the operations of the party in question and sealing its place of operation without delay. The Director of Public Prosecutions and the National Commissioner of the Icelandic Police have the power of prosecution.

3. Law Applicable

The key legislation on data privacy in Iceland is the Data Protection Act.

An English translation of the Act can be found on the DPA’s website, http://www.personuvernd.is/information-in-english/greinar/nr/438

Since the Data Protection Act entered into force, the DPA has issued some public guidelines and rules. Among others are rules on how to obtain an informed consent for processing of personal data in scientific research in the health sector (rules No 170/2001), rules on the obligation to notify and processing of personal data which requires a permit (rules No 712/2008), rules concerning the security of personal data (rules No 299/2001), rules on employers’ supervision of employee’s emails (advertisement No 1001/2001)
4. Key Privacy Concepts

a. Personal Data

Personal data in the Data Protection Act is defined as any data relating to a data subject who is identified or identifiable, i.e., information that can be traced directly or indirectly to a specific individual, deceased or living, according to Article 2. The definition in the Act is based on the standard definition of personal data.

b. Data Processing

Data processing is defined as any operation or set of operations, which is performed upon personal data, whether the processing is manual or automatic, according to Article 2 of the Act.

c. Processing by Data Controllers

Data controllers may process personal data when any of the following conditions are met, according to Article 8 of the Act:

1. the data subject has unambiguously agreed to the processing or given his consent;
2. the processing is necessary to honour a contract, to which the data subject is a party, or to take measures at the request of the data subject before a contract is established;
3. the processing is necessary to fulfil a legal obligation of the controller;
4. the processing is necessary to protect vital interests of the data subject;
5. the processing is necessary for a task that is carried out in the public interest;
6. the processing is necessary in the exercise of official authority vested in the controller or in a third party to whom data are transferred;
7. the processing is necessary for the controller, or a third party, or parties to whom data are transferred, to be able to safeguard legitimate interests, except where overridden by fundamental rights and freedom of the data subject, which shall be protected by law.

Where sensitive personal data is processed, one of the above conditions must be met as well as one of a further list of additional conditions, according to Article 9 of the Act. Those additional conditions are:

1. the data subject gives his consent to the processing;
2. the processing is specifically authorized in another act or law;
3. the controller is required, by contracts between the Social Partners, to carry out the processing;

4. the processing is necessary to protect vital interests of the data subject or of another party who is incapable of giving his consent in accordance with item 1;

5. the processing is carried out by an organization with a trade-union aim or by other non-profit organizations, such as cultural, humanitarian, social or ideological organizations, on condition that the processing is carried out in the course of the organization’s legitimate activities and relates solely to the members of the body or to individuals who according to the organization’s goals are, or have been, in regular contact with it; it is however prohibited to disclose such personal data to a third party without the data subject’s consent;

6. the processing extends only to information that the data subject himself has made public;

7. the processing is necessary for a claim to be established, exercised or defended because of litigation or other such legal needs;

8. the processing is necessary because of a medical treatment or because of the routine management of health care services, provided that it is carried out by an employee of the health care services who is subject to an obligation of secrecy; or

9. the processing is necessary for the purposes of statistical or scientific research, provided that the privacy of individuals is protected by means of specific and adequate safeguards.

d. Jurisdiction/Territoriality

According to Article 6 of the Act, it applies to data controllers and data processors and the processing of personal data: (i) if it is conducted on behalf of a data controller established in Iceland, if the processing is carried out in the EEA, an EFTA country or a country or a place that the DPA lists in a notice in the Law and Ministerial Gazette; (ii) if the data controller, who is established in a country outside of the EEA or EFTA, makes use of equipment and facilities situated in Iceland; and (iii) about financial and credit standing data concerning legal persons using equipment in Iceland even if the data controller is not established in Iceland.

e. Sensitive Personal Data

Sensitive personal data is defined in Article 2 of the Act as the following data:

a. data on origin, skin colour, race, political opinions, religious beliefs and other life philosophies;
b. data on whether a man has been suspected of, indicted for, prosecuted for or convicted of a punishable offence;

c. health data, including genetic data and data on use of alcohol, medical drugs and narcotics;

d. data concerning sex life (and sexual behaviour); and

e. data on trade-union membership.

There are special requirements for processing sensitive personal data, as stated in Section 4(c).

f. **Employee Personal Data**
The Act does not include a specific definition on Employee Personal Data.

5. **Consent**

a. **General**
Consent is the most common ground for processing of personal data. Different requirements are however made in order for consent to be a valid ground, depending on the nature of the personal data being processed.

According to Article 2 of the Data Protection Act, a consent is defined as a specific, unambiguous declaration, which is given freely by an individual, signifying that he agrees to the processing of particular personal data relating to him, and that he is aware of the purpose of the processing, how it will be conducted, how data protection will be ensured, that the individual can withdraw his consent, etc.

As silence is not equivalent to consent, the data subject must be aware of what he is consenting to and what consequences the processing of the information has or can have on him and the data subject must give its consent himself.

Consent regarding processing of general personal data can sometimes be based on active actions on behalf of the data subject. A consent regarding processing of sensitive personal data must however always be in the form of a declaration where the data subject signifies that he/she agrees to the processing in question.

There are no formalities to obtain consent to process personal data under the Act and the Act does not require the consent of the data subject to be in writing unless the processing is for scientific research, according to Article 11 of Rules no 170/2001 on informed consent in scientific research in the health sector.

However, as the consent must be informed, the data subject must be given sufficient information regarding the processing of its personal data and an opportunity to object to it. The burden of proof is placed on the data controller.
to show that this requirement is satisfied. Therefore, for evidential purposes, written consent is recommended in practice.

b. **Sensitive Data**

Sensitive personal data is specifically defined in the Act, as stated in Section 4(e). Processing of sensitive personal data is only allowed if one of the requirements in Article 8 is met as well as one of the requirements in Article 9 of the Act, such as the data subject has given his consent to the processing or the processing is authorized in another act of law.

c. **Minors**

Minors under 18 years old cannot give a valid consent. According to Article 51 of Act No 71/1997 on legal competence, parents of a child not possessing legal competence is in charge of the child’s personal affairs. Consent must therefore be acquired from a child’s parent.

d. **Employee Consent**

There is no specific definition of Employee Personal Data or Employee Consent in the Act. Therefore, the rules in Article 8 and 9, referred to above, apply.

e. **Online/Electronic Consent**

Consent can be given online or electronically, however the consent must fulfill the conditions stipulated in Article 2.

6. **Information/Notice Requirements**

When a data controller obtains personal data directly from the data subject, notice must be provided to the data subject, according to Article 20 of the Act. Notice must also be provided to a data subject when personal data is obtained from someone other than the data subject, according to Article 21.

When a controller obtains personal data directly from the data subject, the following information must be provided to the data subject, according to Article 20 of the Act:

1. the name and address of the controller and, where relevant, its representative in Iceland;
2. the purposes of the processing;
3. other information, in so far as such further information is necessary, having regard to the specific circumstances in which the data is processed, to enable the data subject to protect his or her interests, including information on:
   (a) the recipients or categories of recipients of the data;
(b) whether he is obliged or not to provide the requested data, as well as the possible consequences of failure to reply; and

(c) the provisions of the Act regarding the data subject’s right of access, as well as the data subject’s right to rectification and deletion of wrong or misleading data.

If the data subject has already received this information, it does not need to be provided again.

When personal data is obtained from someone other than the data subject, the controller must concurrently provide the following information to the data subject, according to Article 21 of the Act:

1. the name and address of the controller and, where relevant, its representative in Iceland,

2. the purpose of the processing;

3. other information, in so far as such further information is necessary, having regard to the specific circumstances in which the data is processed, to enable the data subject to protect its interests, including information on:

   (a) the types or categories of the data being processed;

   (b) where the data comes from;

   (c) the recipients or categories of recipients of the data; and

   (d) the provisions of the Act regarding the data subject’s right of access, as well as the data subject’s right to rectification and deletion of wrong or misleading data on it.

When personal data is obtained from someone other than the data subject, a notice is not required if:

1. it is impossible to inform the data subject or if it would place a heavier burden upon the controller than can reasonably be demanded;

2. it may be assumed that the data subject is already aware of the processing;

3. recording or disclosure of the data is laid down by law;

4. the data subject’s interests, of receiving notice of the data, are deemed secondary to vital public or private interests, including its own interests.

There is no obligation to specify the names of the entities or individuals to whom the information is being disclosed. According to DPA practice, the country of the recipients should also be disclosed if the information is to be transferred to recipients established outside of EU/EEA (or outside those
countries or places which the DPA considers to provide adequate level of personal data protection, see Section 11).

7. Processing Rules

When processing personal data, all of the following shall be observed, according to Article 7 of the Act:

1. that they are processed in a fair, apposite and lawful manner and that all their use is in accordance with good practices of personal data processing;
2. that they are obtained for specified, explicit, apposite purposes and not processed further for other and incompatible purposes, but further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that proper safeguards are adhered to;
3. that they are adequate, relevant and not excessive in relation to the purposes for the processing;
4. that they are reliable and kept up to date when necessary, personal data which are unreliable or incomplete, having regard to the purposes for their processing, shall be erased or rectified;
5. that they are preserved in a form which does not permit identification of data subjects for longer than is necessary for the purposes for the processing.

8. Rights of Individuals

Data subjects have the right to be informed of processing of their personal data, whether the data is collected from them or from third parties according to Articles 20 and 21 of the Act, see Section 6.

The data subject can also require the following information from the controller, according to Article 18 of the Act:

1. what data on him is being or has been processed:
2. the purpose of the processing;
3. who receives, has received or will receive data on him;
4. where the data has been obtained;
5. what security measures are applied to the processing, provided that this will not diminish the security of the processing.
However there are a few exemptions from the duty to inform the data subject in Article 19 of the Act. These include data which is solely used for statistical processing or scientific research, provided that the processing cannot have direct influence on the data subject’s interest.

The data subject has the right to request rectification and deletion of incorrect and misleading personal data according to Article 25 of the Act. The data subject can also object, on compelling legitimate grounds relating to his particular situation, to the processing of personal data relating to him, save where otherwise provided by national legislation, according to Article 28 of the Act.

9. Registration/Notification Requirements

Each data controller who uses electronic technology to process personal data must notify the DPA of the processing, using a form intended for that purpose, in a timely manner before beginning the processing, according to Article 31 of the Act. There are no notification costs. Any changes that are made after the original notification shall also be notified.

According to Article 6 of the DPA’s rule No 712/2008 on the obligation to notify and processing of personal data which requires a permit, the following categories of processing of non-sensitive data are exempted from the obligation to notify:

1. processing which is contingent on a permit from the DPA;
2. processing, carried out in the regular or standard course of activities, relating solely to those who have a connection to the activities or the relevant field of work, e.g., business associates, employees, members;
3. processing, necessary to fulfil legal obligations of the controller;
4. processing necessary to fulfil a contract to which the data subject is a party, or an agreement between labor market organizations;
5. processing, extending only to data that has been and is accessible to the public, provided that it is not aligned or combined with other personal data which has not been made accessible; and
6. processing, resulting from electronic surveillance, conducted for the purposes of security and property protection only, provided that legal obligations regarding duty of information and warning have been fulfilled.

The aforementioned exemptions do not apply to the following categories of electronic processing of personal data:

- processing, regarding conduct and individual evaluation, e.g., of performance of employees;
- processing, for the purposes of aligning individuals to personal profiles;
• processing, involving systematic recording of telephone calls.

If the processing of general or sensitive personal data is likely to present specific risks to the rights and freedoms of data subjects, the DPA can decide that the processing may not begin until it has been examined by the DPA and approved, by the issuance of a special permit, according to Article 33 of the Act. The DPA has issued rules No 712/2008 on the obligation to notify and processing of personal data which requires a permit, where it is stipulated when a permit is required for processing of personal data.

Transfer of personal data to countries that do not provide adequate levels of personal data protection is prohibited, unless certain conditions are met, according to Article 30 of the Act. The DPA can however authorize such transfer if it determines that special circumstances warrant it (see Section 11).

10. Data Protection Officers

There is no specific requirement under the Act to appoint data protection officers.

In the event the controller does not have an establishment in Iceland, but the Act is still applicable, the controller must however designate a representative established in Iceland, according to Article 6 of the Act. In such case the provisions of the Act relating to controllers apply to the representative.

11. International Data Transfers

The transfer of personal data to another country that provides an adequate level of personal data protection is permitted, according to Article 29 of the Act. A country that complies with the EU Directive 95/46/EC is considered to provide an adequate level of protection. The same applies to those countries or places which the DPA has listed in advertisement no 228/2010. They are EEA and EFTA member states, Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Jersey, New Zealand, Switzerland, Uruguay, and the Isle of Man, as well as adherents to the US Safe Harbour Principles.

The transfer of personal data to a country that does not provide an adequate level of protection is prohibited, according to Article 30 of the Act, unless:

1. the data subject has consented to the transfer;
2. it is necessary for the fulfilment of obligations under international law or as a result of Iceland’s membership of an international organization;
3. such a transfer is authorized in another legislative act;
4. the delivery is necessary to establish or fulfil a contract between the data subject and the controller;
5. the transfer is necessary to establish or fulfil a contract in the interest of the data subject;
6. the delivery is necessary in order to protect vital interests of the data subject;

7. if dissemination is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or

8. the data in question is accessible to the general public.

The DPA can authorize the transfer of data to a country that does not provide an adequate level of protection, if it determines that special circumstances warrant it, even if the conditions of the provision are not met, according to paragraph 2 of the Article. In such cases the nature of the data, the planned purpose of the processing and its duration are among the factors that must be taken into account. The DPA can authorize the transfer of data to third countries even if they have not been thought of as providing the citizens with an adequate level of privacy protection. This is contingent upon the controller having, in the opinion of the DPA, provided sufficient guarantees to meet these concerns. The DPA can for example require that the controller enter into a written contract with the recipient and that the contract contains certain standard contractual clauses in conformance with a decision which the DPA has advertised in the Law and Ministerial Gazette, having considered the decisions of the Commission of the European Union.

12. Security Requirements

According to Article 11 of the Act, the controller must implement appropriate technical and organizational measures to protect personal data against unlawful destruction, against accidental loss or alteration and against unauthorized access. Having regard to the state of the art and the cost of their implementation, such measures must ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. The controller is responsible for having risk analysis and security measures which are implemented in the processing of personal data, conform with laws, rules and instructions given by the DPA on how to ensure information security, including standards that the DPA decides that must be followed. The controller is responsible for risk analysis being reviewed routinely and security measures upgraded to the extent necessary to fulfil these security requirements. The controller must document how he produces a security policy, conducts a risk analysis and decides on security measures to be implemented. The DPA must be granted access to information regarding these issues at any time.

Where data is to be processed by a processor, the controller must ensure that the processor in question is able to carry out the required security measures and conduct internal audits, according to Article 13 of the Act.
13. Special Rules for the Outsourcing of Data Processing to Third Parties

When processing is carried out by a processor, the controller must verify that the processor in question is able to carry out the required security measures and conduct internal audits, according to Article 13 of the Act. The controller must enter into a written agreement with the processor with specific obligations, i.e.,:

- that the processor must act only on instructions from the controller and that the obligations set out in the Act will also be incumbent on processing carried out by the processor;
- anyone acting in the name of the controller or the processor, including the processor itself, and has access to personal data, may only process personal data according to the instructions of the controller, unless legislative acts stipulate otherwise;
- if the processor is established in another state within the European Economic Area than the controller, then it must also be stipulated in the contract that the laws and regulations of the state in which the processor is established will govern the security measures to be applied to the processing of personal data.

14. Enforcement and Sanctions

The DPA is responsible for the enforcement of the Data Protection Act, according to Article 37 of the Act.

Infringements of the provisions of the Act and of regulations issued according to it are punishable by means of fines or a prison term of up to three years, unless more severe sanctions are provided for in other acts of law, according to Article 42 of the Act. The same punishment does apply if instructions by the DPA are not observed. If an offense is committed as part of the operations of a legal person, that legal person can be fined, as provided for in Chapter II A of the General Penal Code.

If a controller or a processor has processed personal data in violation of the Act, rules or instructions by the DPA, then the controller must compensate the data subject for the financial damage suffered by it as a result of this, according to Article 43 of the Act. A controller will, however, not be made to compensate for any detriment which it proves that can neither be traced to its mistake nor to any negligence on its or its processors’ behalf.

The DPA can order the cessation of processing of personal data, including collection, documenting or disclosure, order the erasure of personal data or the deletion of records, wholly or partially, prohibit further use of data or instruct the controller to implement measures that ensure the legitimacy of the processing, according to Article 40, paragraph 1 of the Act.
If a processing is discovered, which violates provisions of the Act, or those administrative rules which are issued according to it, the DPA can assign to the Chief of Police the task of halting temporarily the operations of the party in question and seal its place of operation without delay, according to Article 40, paragraph 2 of the Act.

If someone does not comply with the above mentioned instructions of the DPA, then it can revoke a permit that it has granted according to the provisions of the Data Protection Act until it concludes that the necessary improvements have been made, according to Article 40 of the Act.

15. Data Security Breach
There is no mandatory requirement in the Data Protection Act to report data security breaches or losses to the DPA or to the data subject.

However, a notice is considered as good practice, particularly if the security breach is major.

16. Accountability
The controller shall ensure that the processing of personal data is always in compliance with the Act. A processor can also be held liable.

17. Whistle-Blower Hotline
There are no obligations or regulations specific to whistleblowing hotlines; however, the general data protection rules would apply with respect to the processing of any personal data that results from the establishment of such hotlines. It may be expected that the DPA would take note of Opinion 1/2006 of the Article 29 Data Protection Working Party when interpreting general provisions of the Act.

18. E-Discovery
There are no special rules in Iceland regarding E-Discovery.

19. Anti-Spam Filtering
There are no special rules in Iceland regarding Anti-Spam Filtering.

20. Cookies
There are no provisions in Icelandic legislation which particularly deal with the use of cookies or location data. IP addresses are considered personal data as well as location data. If the use of cookies leads to the use of IP addresses, or other personal data, the processing of such data and location data must comply with the Act. The processing is therefore not permissible unless one of the listed conditions is met, in most instances the data subject must consent to the processing of such data.
21. Direct Marketing

Based on the ECA the use of automated calling systems, including electronic mail, for direct marketing is only allowed if a subscriber has given prior consent, according to Article 46 of the ECA. If the electronic mail addresses have been obtained in the context of the sale of a product or service it may be used for direct marketing of own goods or services if customers are given the opportunity to object to such use of addresses free of charge when they are listed and similarly each time a message is sent, if the customer has not initially refused such use.

Apart from that, unsolicited electronic communications in the form of direct marketing are not allowed for subscribers who do not wish to receive these communications.

The sending of electronic mail for purposes of direct marketing, where the name and address of the party responsible for the marketing is not clearly indicated, is prohibited, according to Article 46 of the ECA.

Registers Iceland, which registers a range of information on Iceland’s residents and real properties, also maintains a registry of those individuals who object to their names being used for marketing purposes, according to Article 28 of the Data Protection Act. Controllers engaged in direct marketing, and those who use a list of names, addresses, e-mail addresses, phone numbers and similar data, or disclose them to a third party in connection with a similar enterprise, shall, prior to using such a list for the described purposes, compare it with the Registers Iceland’s registry, in order to prevent direct mail from being sent to, or phone calls being made to, those who have objected to it. The DPA can make exemptions from this duty in special cases.
India

Probir Roy Chowdhury
Bangalore
Tel: +91-80-43503618
probir@jsalaw.com

Sajai Singh
Bangalore
Tel: +91-98450 78666
sajai@jsalaw.com
1. Recent Privacy Developments

Mandatory Notification of Data Security Incidents

The Government of India has enacted the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (“Cert-In Rules”), which impose mandatory notification requirements on service providers, intermediaries, data centers and corporate entities, upon the occurrence of certain ‘cyber security incidents’.

Cyber security incidents have been defined to mean any real or suspected adverse events, in relation to cyber security, that violate any explicitly or implicitly applicable security policy, resulting in:

- unauthorised access, denial or disruption of service;
- unauthorised use of a computer resource for processing or storage of information; or
- changes to data, information without authorisation.

The occurrence of the following types of cyber security incidents trigger the notification requirements under the Cert-In Rules:

a. Targeted scanning/ probing of critical networks/ systems;
b. Compromise of critical information/ system;
c. Unauthorized access of IT system/ data;
d. Defacement of websites or intrusion into website of unauthorized changes such as inserting malicious codes, links to external websites;
e. Malicious code attacks such as spreading virus, worm/trojan/botnets/ spyware;
f. Attacks on servers such as database, mail and DNS & network devises such as routers;
g. Identity theft, spoofing and phishing attacks;
h. Denial of service (DoS) and Distributed Denial of service (DDoS) attacks;
i. Attacks on critical infrastructure, SCADA systems and wireless networks; and
j. Attacks on applications, such as E-governance and E-commerce etc.

Upon the occurrence of any of the aforementioned events, companies are now required to notify the Computer Emergency Response Team (CERT-In) within a reasonable time, so as to leave scope for appropriate action by the authorities. The format and procedure for the reporting of cyber security
incidents have been provided by Cert-In on its official website, http://www.cert-in.org.in/.

CERT-In was established in 2004, to collect, analyse and disseminate information on cyber incidents, provide forecasts and alerts of cyber security incidents, provide emergency measures for handling cyber security incidents and coordinate cyber incident response activities.

2. Emerging Privacy Issues and Trends

Right to Privacy Bill, 2011

2015 is anticipated to be the year when the Government of India introduces the Right to Privacy Bill, 2011 (“Privacy Bill”) in the Parliament for scrutiny and approval. The Privacy Bill proposes an overhaul of the data privacy framework in India, whereby the collection, storage, processing and transfer of data would be assessed for compliance through the lens of privacy principles (similar to the OECD privacy principles). The Privacy Bill also proposes the setting up of a Data Protection Authority (“DPS”), to investigate any data security breaches and issue appropriate orders to safeguard security interests of all affected data subjects. It also proposes to provide guidance for data controllers, who would be responsible for exercising self regulation and confidentiality while dealing with personal data. In June 2014, the Department of Personnel and Training (“DoPT”) submitted the Privacy Bill to the Ministry of Law and Justice for its consideration. If approved, the Privacy Bill would be sent to the Cabinet of Ministers for a final review, and thereafter placed before the Parliament of India for enactment.

3. Law Applicable


The following additional legislations, though not directly dealing with data protection and information technology, find application in addition to the aforementioned regulations:

(i) The Indian Contract Act, 1872;
(ii) Indian Penal code, 1860;
(iii) Right to Information Act, 2004;
(iv) Indian Copyright Act, 1957;
(v) The Consumer Protection Act, 1986;
(vi) Specific Relief Act, 1963;
(vii) Reserve Bank of India Act, 1934;
(viii) Tort Law.

Offenses under the above rules and regulations are enforced by the judiciary and the various cyber crime cells across the country. The provisions of the Indian Penal Code, 1860, have been applied to offenses under the law applicable to information technology as well. India does not have a ‘Regulator’ in place presently, however there are various organizations lobbying for more stringent data protection and privacy laws to be implemented. Presently, data protection is maintained by the judiciary and the cyber crime units of the police force.

4. Key Privacy Concepts

a. Personal Data

The Privacy Rules define “Personal Data” as “any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.”

Apart from Personal Data, the Privacy Rules also define the term “Sensitive Personal Data or Information”. Even though both the terms have been defined in the Privacy Rules, the concepts tend to overlap. Different provisions are applicable to “Personal Information” and “Sensitive Personal Data or Information”, while some provisions are applicable to both. The interpretation of the Press Note and the current stance of the industry is that, while all the provisions of the Privacy Rules apply to Sensitive Personal Data or Information, only some provisions apply to Personal Data or Information.

b. Data Processing

Person located in India

Privacy Rules are applicable to a person located in India. However, there is lack of clarity on whether the term "person" refers to “natural individuals” who are the providers of information, or body corporates collecting data.

If it is assumed that “person” refers to “natural individuals”, then a body corporate located overseas, which handles data of individuals located in India through a computer resource located in India, will have to comply with the Privacy Rules.

Body corporate located in India, computer resource located in India or overseas

Irrespective of the location of the computer resource (either in India or abroad) and the place of residence of the data subject, the Privacy Rules are applicable to all body corporates located in India.
Body corporate located overseas, computer resource located in India

Section 43-A of the IT Act, read with Section 75, provides that the IT Act will be applicable to a body corporate located overseas, whose computer resource is located in India. As per the interpretation that has been adopted, the Privacy Rules apply to all Indian body corporates and to those foreign body corporates which collect personal or Sensitive Personal Data or Information from Indian persons.

c. Processing by Data Controllers

There are no specific provisions under applicable Indian laws.

d. Jurisdiction/Territoriality

A body corporate or any person on its behalf may transfer Sensitive Personal Data or Information or any other information, to any other body corporate or a person in India, or in any other country, only after it ensures, in the case of another country, that such jurisdiction provides the same level of data protection as is required to be in compliance with the Privacy Rules. Further, such transfer may be done only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and Data Subject. Alternatively, such data may be transferred with prior consent of the Data Subject. As per the accepted interpretation of the Privacy Rules, this provision is applicable for both personal and Sensitive Personal Data or Information.

e. Sensitive Personal Data

The Privacy Rules define sensitive personal information to include information relating to:

- passwords;
- financial information (e.g., bank account/credit or debit card or other payment instrument details);
- physical, physiological and mental health condition;
- sexual orientation;
- medical records and history;
- biometric information (biometrics means the technologies that measure and analyse human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA for authentication purposes);
- any detail relating to the above clauses as provided to a body corporate for providing services; and
any of the information received under the above clauses for storing or processing under a lawful contract or otherwise.

However, any information available in the public domain or any information to be furnished to any government agency or which should be made available to the public under the Right to Information Act, 2005 has been expressly exempt from the scope of this definition.

f. Employee Personal Data

There are no additional requirements/definitions for employee Personal Data. If Sensitive Personal Data or information of employees is being collected, then prior consent of such employees will be required.

There is no specific legislation pertaining to monitoring of employees. Employers do monitor email and computer use of employees but usually inform employees about such monitoring. Employers must be careful to comply with the right to privacy of employees and comply with regulations pertaining to collection, use, storage and transfer of Sensitive Personal Data and Personally Identifiable Information. Further, the IT Act also regulates images being captured via such monitoring and employers would have to adhere to the same.

An additional point to be noted is that the courts may construe the right to access information on a computer or computer resource in light of the ownership of computer or computer resource being transferred.

5. Consent

a. General

In India, consent of the Data Subject is required for the collection, processing, and disclosure of Personal Data. Consent is also contemplated as a justification or legal grounds for the collection, processing and/or use of Personal Data.

For consent to be considered valid, it must be voluntary, informed, explicit and unambiguous. It can be express or implied but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. Consent must be obtained prior to or at the time of collection of data. Consent given by a Data Subject can be withdrawn at any time. It does not need to be in the local language, but the Data Subject must understand the language in which consent is given.

b. Sensitive Data

An organization that processes Sensitive Data has an obligation to obtain consent in writing through letter or fax or email or other electronic means from the Data Subject.
Based on this, the privacy policy of each body corporate may contain an “I Agree” tab at the end of the text. A click on the tab by the reader of the privacy policy (i.e., the Data Subject) would be deemed to be valid consent under the Privacy Rules.

Additionally, the Privacy Rules require that, while collecting Sensitive Personal Data or information directly from the Data Subject, the body corporate must, inter alia, inform the Data Subject of the purpose for which his or her information is being collected, that the information so collected may be transferred/disclosed and names/addresses of the agency collecting and retaining this information.

Further, a body corporate or any person on its behalf may collect any Sensitive Personal Data or information only if the information is collected for a lawful purpose connected with an integral activity of the body corporate.

c. Minors

There are no specific guidelines with regard to data privacy under the IT Act or Privacy Rules regarding minors.

However, the IT Act punishes publication or transmission of material depicting children in sexually explicit acts, in electronic form.

d. Employee Consent

Employee consent is required to collect and process an employee’s Personal Data.

Employee consent is required if his or her sensitive Personal Data or information is being collected, used, handled, stored and/or transferred by the employer (i.e., the body corporate). The requirements for such consent are the same as the general consent requirements.

Employee consent is also required when an employer decides to implement a BYOD program. There is no specific legislation pertaining to BYOD, however various laws pertaining to the right to individual privacy and collection and storage of Sensitive Personal Data and personally identifiable information would apply. The general practice prevalent is for companies to implement in-house corporate policies that cover various scenarios regarding confidentiality, integrity and access of data.

e. Online/Electronic Consent

Online/Electronic consent is permissible and can be effective if properly structured and evidenced. Hence, electronic consent is enforceable in India.

The related contract must comply with the requirements of the Indian Contract Act, 1872 to qualify as valid binding contracts.
The IT Act prescribes regulations pertaining to electronic signatures, the procedure for the issuance and the manner of obtaining a digital signature, and regulations pertaining to certifying authorities. Under the IT Act, any subscriber may authenticate an electronic record by affixing his digital signature to such electronic record.

Further under the Indian Evidence Act, 1872 electronic records may be submitted as primary evidence if compliant with the conditions provided thereunder. However the prevalent practice presently is to affix a ‘wet signature’ to a document, scan and email the same as an electronic record. This does not however satisfy the conditions provided under the Evidence Act, 1872 for electronically signed documents and primary evidence and is thereby considered secondary evidence by the courts.

6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred and stored; how to contact the privacy officer or other individual who is accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; how to access/and or correct the Data Subject’s Personal Data; the duration of the proposed processing; and the means of transmission of the Personal Data.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/ anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

There are no formal registration requirements in India imposed on organizations that collect and process Personal Data.
10. Data Protection Officers
Every body corporate collecting/ using/ retaining or transferring Sensitive Personal Data or information is obligated to designate a Grievance Officer in order to address any discrepancies and/or grievances that any Data Subject may have. The names and contact details of such Grievance Officer must be published on the website of the body corporate. The Grievance Officer is required to redress the grievances of the Data Subject within one month from the date of receipt of grievance.

11. International Data Transfers
Organizations in India may transfer Personal Data outside of the jurisdiction provided that the receiving jurisdiction provides a similar level of protection for Personal Data; impacted Data Subjects have been informed or have been provided consent; and that reasonable steps have been taken to safeguard the Personal Data to be transferred.

12. Security Requirements
Organizations are required to take steps to: ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

Foreign entities may have to comply with Indian security standards when dealing with Indian companies. Presently, Indian legislation prescribes data security standards of ISO/IEC 27001:2005 as the norm when handling sensitive personal information and personally identifiable information.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data. These organizations may also be required to comply with sector specific requirements. Furthermore, organizations that outsource data processing shall be liable with the third party provider in case of breach by the latter.

There is no specific regulation pertaining to cloud computing. However any entity collecting Sensitive Personal Data or personally identifiable information must comply with ISO/IEC 27001:2005 security standards.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, civil actions, and/or private rights of action. As per the IT Act, any body corporate which breaches Section 43-A is liable to pay damages by way of compensation to the Data Subject so affected. There is no limit on the amounts recoverable.
15. Data Security Breach
As discussed earlier, under the Cert-In Rules, service providers, intermediaries, data centers and corporate entities are obligated to notify Cert-In upon the occurrence of certain cyber security incidents, including data security breaches. While no fixed time limit has been prescribed in this regard, the Cert-In Rules require such notifications to be made within such reasonable time as would allow authorities to take necessary remedial measures.

16. Accountability
Organizations are currently not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-blower hotline
There is no filing requirement for the introduction of a whistle-blower hotline in India. Whistle-blower hotlines may be established as long as they are in compliance with local laws.

18. E-discovery
When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of Personal Data is involved, and advise employees of its implementation, the monitoring of work tools, and the storage of information.

19. Anti-Spam Filtering
Generally, the introduction of a spam filtering solution in an organization does not raise privacy issues provided that the employees have been informed of the monitoring policies being implemented in the workplace.

20. Cookies
There are specific laws/rules that regulate the deployment of cookies in India; and hence, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted. Consent of Data Subjects must be obtained before cookies can be used.

Under the IT Act, any person who, without permission of the owner or any other person who is in charge of a computer, computer system or computer network or computer resource introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network shall be liable to pay damages by way of compensation to the person so affected.
Cookies fall under the definition of ‘computer virus’ as provided under the IT Act which means any computer data that attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

Based on the above, if a person were to include cookies on their websites without obtaining permission of and informing such user of the use of cookies and any damage were to result from the placement of such cookies, the owner of such website would be liable to pay compensation to the person so effected.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.

There is no specific legislation in India that governs online direct marketing; however, the general practice is to permit an intended recipient to opt-in/opt-out of receiving any marketing material.

There is no existing legislation that governs spam, however the general practice of providing an opt-in/unsubscribe option is followed by email marketers. The IT Act has tried to implement anti-spam regulations which state that any person who sends by means of a computer resource or a communication device, any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages may be punishable with imprisonment for a term which may extend to three years and with fine. Any information that may be grossly offensive, have menacing character, cause annoyance, inconvenience, danger, obstruction, insult, injure, criminally intimidate, cause enmity, hatred or ill will, sent persistently by use of a computer resource or a communication device may be held in violation of the IT Act.

This provision has not however been tested in a court of law and does not specifically deal with email marketing.

The Telecom Commercial Communications Customer Preference Regulations (“TRAI Regulations”) regulate unsolicited marketing calls. The TRAI Regulations establish a ‘National Do Not Call Register’, and a ‘Private Do Not Call List’. The TRAI Regulations provide customers with the option to register with Telecom Regulatory Authority of India (“TRAI”) or their service providers under the ‘fully blocked’ or ‘partially blocked’ categories. The TRAI Regulations also require telemarketers to register themselves with TRAI which maintains a National Telemarketers Register.
Indonesia

Aryadharma Alimsardjono
Jakarta
Tel: +62 21 2960 8501
aryadharma.alimsardjono@bakermckenzie.com

Susie Beaumont
Jakarta
Tel: +62 21 2960 8608
susie.beaumont@bakermckenzie.com

Mark Innis
Jakarta
Tel: +62 21 2960 8618
mark.innis@bakermckenzie.com

Alvira M. Wahjosoedibjo
Jakarta
Tel: +62 21 2960 8503
alvira.m.wahjosoedibjo@bakermckenzie.com
1. Recent Privacy Developments

There have been no recent significant developments on data privacy in Indonesia. There are still no specific data privacy/protection regulations in Indonesia.

However some regulations are expected in late 2015.

2. Emerging Privacy Issues and Trends

**Wire-tapping Issues & Security requirements** – After the recent government wire-tapping issues by other countries, the Ministry of Communications and Informatics (“MOCI”) indicates that they will tighten the data privacy requirements (especially for telecommunication operators) in Indonesia. Recently, the MOCI issued a directive to major Indonesian telecommunication companies to provide reports on wire-tapping procedures and mechanisms, and will require stricter security requirements including the protection of privacy of the customers.

**Data Protection Enforcement** - In the absence of a specific data protection/privacy regulation, the implementation of data privacy requirements in Indonesia is limited. The MOCI will issue a ministerial regulation on Personal Data protection/privacy. However, there is no draft regulation available and the MOCI cannot confirm when such regulation will be issued.

3. Law Applicable

Law No. 11 of 2008 on Electronic Information and Transaction (“EIT Law”) and Government Regulation No. 82 on the Implementation of Electronic Systems and Transactions (“Regulation 82”) remain the main law and regulation that address data protection/privacy matters.

Other than the above, there are also a number of other Indonesian laws that relate to the issue of data privacy (e.g., bank secrecy requirements under the banking regulations).

4. Key Privacy Concepts

**a. Personal Data**

Regulation 82 defines “Personal Data” as data of individuals which must be stored and maintained without error and the secrecy of which is protected (this is a literal translation of the regulation and it remains unclear at this time).

The above definition only covers data of individuals and does not cover data on businesses (e.g., company’s name, address, phone number, etc.). However, the definition is very general and may be interpreted broadly. It is advisable that a conservative approach be taken in assessing whether certain data contains Personal Data and to assess whether or not an element of information can lead to a specific person (e.g., name, email, IP address, phone number, ID, location, etc.).
b. Data Processing
Effectively, data processing the use of Personal Data, which must be based on consent from the Data Subject and in accordance with the purpose conveyed to the relevant Data Subject when collecting the data.

c. Processing by Data Controllers
There are no specific laws or regulations on the processing of Personal Data by Data Controllers. Effectively, any use of Personal Data must be based on consent from the Data Subject and in accordance with the purpose conveyed to the relevant Data Subject when collecting the data.

d. Jurisdiction/Territoriality
The EIT Law (including, in this regard, Regulation 82 as its implementing regulation) applies to local or foreign legal subjects and to all electronic transactions conducted inside or outside Indonesia, having a legal impact in Indonesia, or having a legal impact outside of Indonesia but produces detrimental effects to the interests of Indonesia.

Consequently, entities which do not have any presence in Indonesia but have activities that may affect Indonesia or Indonesian entities/individuals, may also be subject to the EIT Law. Although, in practice the EIT Law has not been strictly enforced against an offshore entity given the impracticality of doing so, ultimately the Government could require sites/services to be blocked (as it does with pornography sites).

e. Sensitive Personal Data
There is no law or regulation which classifies certain Personal Data as Sensitive Personal Data. In practice, however, the consent form, employment agreement, company regulation or collective labor agreement may include a provision which classifies certain Personal Data of an employee as “Sensitive Personal Data of an employee”.

f. Employee Personal Data
There is no law or regulation which classifies certain data of an employee as Personal Data. In practice, however, the consent form, employment agreement, company regulation or collective labor agreement may include a provision which classifies certain data of an employee as employee Personal Data.

5. Consent
a. General
The EIT Law and Regulation 82 require consent of the relevant individuals with respect to any use of their private or Personal Data through electronic media and/or electronic systems, unless the law stipulates otherwise. In addition, there is ambiguity among the various Indonesian laws to suggest that the prudent course would be to always secure prior consent of the Data
Subject of such data to use, process, transfer and disclose their Personal Data, regardless of whether electronic media are used.

b. Sensitive Data
There is no provision in the EIT Law, Regulation 82 or other laws and regulations on “Sensitive Data”. As the EIT Law and Regulation 82 generally require consent for any use of Personal Data in electronic media and/or electronic systems from the relevant Data Subjects, any use of Sensitive Personal Data must also be based on prior consent of the owner of such Sensitive Data.

c. Minors
There is no provision in the EIT Law, Regulation 82 or other laws and regulations specifically addressing consent requirements for the use of a minor’s data. However, consent may be obtained from a legal guardian or parent on behalf of a minor.

d. Employee Consent
The EIT Law requires consent of the relevant individuals with respect to any use of their private or personal information through electronic media, unless the law stipulates otherwise. Regulation 82 requires Electronic Systems Operators to ensure that the use of Personal Data (including employees) is based on consent. In practice, the employment agreement, company regulation or collective labor agreement may also include a provision which reflects the employees consenting to the employer’s possible use, access, process, transfer and disclosure of their Personal Data. Nevertheless, in reviewing a number of related laws, the prudent course of action is to secure the prior consent of the employees concerned regardless of whether electronic media are used.

e. Online/Electronic Consent
Technically, it is possible to obtain affirmative/express consent of a Data Subject online or electronically. Under the EIT Law and Regulation 82, electronic information and electronic documents, including their print outs, are considered valid legal evidence, except where the law requires such documents to be made in writing (e.g., employment agreements) or in the form of a deed (e.g., land title documents). Electronic information and electronic documents are valid to the extent that the information can be accessed, presented or guaranteed of its completeness, and can be relied on to explain certain situations.

In practice, Indonesian courts (particularly, the Industrial Relations Courts, in the event of an employment dispute) may request for a print-out of the relevant electronic document.
In light of the above, we suggest that even though consent can be obtained electronically, mechanisms are put in place to:

(i) allow the printing of such consent whenever necessary (e.g., in the event that the consent will be used as evidence in court); and

(ii) verify the authenticity of the consent (which is electronically generated).

6. Information/Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to make an inquiry or file a complaint, how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization on what Personal Data is being collected and how the Personal Data is being used; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

There are no requirements for organizations that collect and process Personal Data to register, file or notify the local data authority.

10. Data Protection Officers

There is no requirement for organizations to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.
11. International Data Transfers
Organizations may transfer Personal Data outside of Indonesia provided that impacted Data Subjects have been informed or have provided consent; and that reasonable steps have been taken to safeguard the Personal Data to be transferred.

12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
The general requirements of an outsourcing arrangement under the Indonesian labor laws and regulations will apply.

In addition, for Indonesian banks, the Central Bank has Bank Indonesia Regulation No. 9/15/PBI/2007 on the Application of Risk Management System for Information Technology in Banks. This regulation is the legal basis for banks in Indonesia in applying its information technology system, particularly for data processing.

Indonesian banks are allowed to engage a third party that provides Information Technology service. The Information Technology service provider may be a local provider (Indonesian company) or a foreign provider (non-Indonesian company). If the bank intends to engage a foreign Information Technology service provider, the bank must first secure an approval from Bank Indonesia (Indonesia’s Central Bank).

Such approval can only be given by Bank Indonesia, if the Indonesian bank meets certain requirements.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, administrative fines, penalties or sanctions, civil actions, class actions, criminal proceedings, and private rights of action.

15. Data Security Breach
Regulation 82 requires a written notification to the relevant Data Subject in case of a data breach.
An organization that is involved in a data breach situation may be subject to a suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, or civil actions and/or class actions, and a criminal prosecution.

16. Accountability

Subject to regulatory guidance, organizations may be required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data; furnish the results of the privacy impact assessments to privacy regulators upon request; and furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.

17. Whistle-Blower Hotline

There are no laws/rules that regulate the implementation of whistle-blower hotlines in Indonesia.

18. E-Discovery

A provision in the Human Rights Law provides that secrecy of correspondence (including those in electronic form) may not be violated except by a court order in accordance with the prevailing laws. In addition, under the EIT Law, the basic principle is for the confidentiality of private or personal information of an individual must be preserved. Conceivably, if Personal Data of employees are deemed to have been gathered from various correspondence between the company and its employees, the provisions under the Human Rights Law and the EIT Law may be applied. However, there has been no case reported on this.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace; and give employees the opportunity to review the isolated emails designated as spam.

20. Cookies

There are no specific laws/rules in Indonesia that regulate the use and deployment of cookies.

21. Direct Marketing

An organization that plans to use any Personal Data for direct marketing activities is required to obtain the Data Subject’s prior consent.
Ireland

John Cahir
Dublin
Tel: +353 1 649 2000
jcahir@algoodbody.com

Alison Obernik
Dublin
Tel: +353 1 649 2461
aobernik@algoodbody.com
1. Recent Privacy Developments


- On 18 July 2014, the remaining provisions of the DP Acts were signed into effect by the Minister for Justice and Equality. S.I. No. 337 of 2014 brought subsections 6(2)(b) and 10(7)(b) into effect, while S.I. No. 338 of 2014 brought into force subsection 4(13) of the DP Acts.

- Section 6 had already provided that a Data Controller must rectify, block or erase personal data that is collected, processed or otherwise dealt with in contravention of the DP Acts and to notify the data subject accordingly. Section 6(2)(b) extends this obligation by requiring a data controller to notify any person to whom personal data was disclosed to in the 12 preceding months. There is an exception for when such notification proves impossible or involves a disproportionate effort.

- Section 10 had already provided that following receipt of an enforcement order issued by the Office of the Data Protection Commissioner (“ODPC”), the data controller must notify the data subject where the controller blocks, rectifies, erases, destroys or adds a statement to personal data. Section 10(7)(b) extends this obligation by requiring the data controller to also notify any person to whom the personal data was disclosed during the preceding 12 months. The same exception applies in relation to when the notification proves impossible or involves a disproportionate effort.

- Section 4(13) makes it unlawful for employers to require employees or job applicants to make an access request seeking copies of personal data which is then made available to the employer/prospective employer. This subsection also applies to any person who engages another to provide a service. In June 2015 the ODPC announced that it had written to 40 organisations across a range of industries so as to assess their compliance with legislation on enforced subject access requests.

ODPC secured first personal convictions against company directors

- In October 2014, the ODPC secured its first personal convictions against company directors for their part in the breach of data protection law by their private investigation company. The company was charged with 23 counts of breaches of section 22 of the DP Acts for obtaining access to personal data without the prior authority of the data controller by whom the data is kept and disclosing the data to another person. Separate prosecutions were made under section 29 of the DP Acts, which provides for the prosecution of directors, or other officers of a company, where an offence by a company is proved to have been committed with the consent
or connivance of or to be attributable to any neglect on the part of the directors or other officers.

**Increased Government Focus on Data Protection**

- The 2015 Irish Government Budget doubled the funding for the ODPC. In July 2014, Ireland appointed Dara Murphy TD as a dedicated Data Protection Minister. In December 2014, Minister Murphy took part in the Irish Government’s filing of an *amicus curiae* brief in relation to the US Court of Appeal case *Microsoft v the United States*. *Amicus curiae* (friend of the court) standing allows a party to offer perspective and a position on a case that it is not directly involved in. The brief outlined the Irish position with regard to the ongoing legal dispute between the US and Microsoft over access to an email account held on an Irish server.

- 2014 also saw the replacement of former Data Protection Commissioner, Billy Hawkes with Ireland’s first female Data Protection Commissioner; Helen Dixon. Amongst her proposals for 2015 is an increased focus on the level of clarity and information given to the data subjects by public bodies that process and control data.

2. **Emerging Privacy issues and Trends**

**Cyber Crime and Cyber Security**

- Ireland is required to transpose Directive 2013/40/EU on Attacks against Information Systems by 4 September 2015. The Directive retains most of the provisions contained in the EU’s first legal initiative in this area; Council Framework Decision 2005/222/JHA. However, in response to the evolution and sophistication of cybercrime, the Directive has introduced new crimes such as botnet attacks (the use of a group of computers or servers for malicious purposes) and identity theft. An obligation has also been imposed on Member States to respond to urgent information requests within eight hours and to collect basic statistical data on national cybercrime including the number of offences registered and the number of persons convicted.

- This area of cyber security also continues to grow in Ireland as cyber threats are now seen to be as tangible as physical threats to a company’s assets with companies needing to focus on the ever-changing set of laws and regulations relating to the collection, storage and use of data. The PWC 2014 Irish Economic Crime Survey stated that the instances of reported cybercrime have doubled in the last two years, while it remains the second most common type of fraud after asset misappropriation. In line with this new threat, there has been an increase in the amount of companies purchasing cyber-insurance in an effort to cope with the risks posed by cybercrime. The insurance is aimed at alleviating some of the associated costs victims of cybercrime security breaches face such as
the expense of notifying clients, IT forensics experts' fees and possible ODPC fines.

**Data Protection Audits**

- In August 2014, the ODPC published an updated version of their 2009 Guide to the Audit Process. The revised version was updated to reflect the developments in the legislation and the changes in the approach of the ODPC to the audit process. The guide is aimed at assisting those who are selected for audit by the ODPC.

- 2014 saw a 13% decrease in the number of audits from 2013 to 38. The legal basis for the audits, which the ODPC has conducted since 2003, is contained in Section 10 (1A) of the DP Acts. The audits usually involve the examination of an organisation's records, systems, policies and procedures in order to assess whether the organisation is generally in compliance with requirements under the DP Acts. The audit will also involve the review of the organisation’s general level of awareness of the requirements under the DP Acts based on the existing policies and practices of the organisation.

3. Law Applicable


- The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, implemented the E-Privacy Directive 2002/58/EC.

4. Key Privacy Concepts

a. **Personal Data**

The DP Acts apply to the processing of any data (“Personal Data”) relating to an identified or identifiable living individual (“Data Subject”). Personal Data is defined under the DP Acts as data relating to a living individual who is or can be identified either from the data or, most notably, from the data in conjunction with other information that is in or is likely to come into, the possession of the data controller. Where the disclosure or receipt of data does not include Personal Data as defined then such processing falls outside the scope of the legislation.

The ODPC has issued guidance that in order for the processing of Personal Data to be considered fair for the purposes of the DP Acts certain information must be provided to an individual. It covers any information that relates to an identifiable, living individual. There are different ways in which an individual can be considered ‘identifiable’. A person’s full name is an obvious likely identifier but a person can also be identifiable from other information, including
a combination of identification elements such as physical characteristics, pseudonyms, occupation, or an address.

b. Data Processing

“Processing” is widely defined to mean performing any operation or set of operations on information or data, whether or not by automatic means. To ensure that processing is in accordance with the DP Acts, a Data Controller should obtain consent from a Data Subject to process his/her Personal Data and should give notification to the Data Subject of certain specified information. This would include information on the right of access to the Personal Data and the purposes for which the data are processed.

c. Processing by Data Controllers

The DP Acts apply to a person who, either alone or with others, controls the contents and use of Personal Data (a “Data Controller”).

d. Jurisdiction/Territoriality

The DP Acts apply to Data Controllers in respect of the processing of Personal Data only if:

- the Data Controller is established in Ireland and the data is processed in the context of that establishment, or
- the Data Controller is established neither in Ireland nor in any other state that is a contracting party to the European Economic Area (EEA) Agreement but makes use of equipment in Ireland for processing the data otherwise than for the purpose of transit through the territory of Ireland.

The following shall be treated as “established in Ireland”:  

- an individual who is normally resident in Ireland,
- a body incorporated under the law of Ireland,
- a partnership or other unincorporated association formed under the law of Ireland, and
- a person who does not fall within the above, but maintains in Ireland an office, branch or agency through which he or she carries on any activity, or a regular practice.

e. Sensitive Personal Data

Sensitive Personal Data means Personal Data relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health or condition, sexual life, commission or alleged commission of any offence, or criminal proceedings. The DP Acts set out additional requirements for the processing of sensitive Personal Data.
The processing of Sensitive Personal Data is prohibited unless at least one of a number of stated conditions is met.

- the Data Controller obtains the explicit consent of the Data Subject;
- the processing is necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the Data Controller in connection with employment;
- the processing is necessary to prevent injury or other damage to the health of the data subject or another person or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the Data Subject or of another person in a case where consent cannot be given by or on behalf of the Data Subject or where the Data Controller cannot reasonably be expected to obtain such consent, or the processing is necessary to prevent injury to, or damage to the health of, another person, or serious loss in respect of, or damage to the property of another person, in a case where such consent has been unreasonably withheld;
- the processing is carried out in the course of its legitimate activities by any body corporate, or any unincorporated body of persons, that is not established, and whose activities are not carried on, for profit, and exists for political, philosophical, religious or trade union purposes, it is carried out with the appropriate safeguards for the fundamental rights and freedoms of Data Subjects, it relates only to individuals who are either members of the body or have regular contact with it in connection with its purposes and it does not involve disclosure of the data to a third party without the consent of the Data Subject;
- the information contained in the data has been made public as a result of steps deliberately taken by the Data Subject;
- the processing is necessary for the administration of justice, for the performance of a function conferred on a person by or under an enactment, or for the performance of a function of the Government or a Minister of the Government;
- the processing is required for the purpose of obtaining legal advice or for the purposes of, or in connection with, legal proceedings or prospective legal proceedings, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- the processing is necessary for medical purposes and is undertaken by a health professional, or a person who in the circumstances owes a duty of confidentiality to the Data Subject that is equivalent to that which would exist if that person were a health professional;
• the processing is necessary in order to obtain information for use, subject to and accordance with the Statistics Act, 1993, only for statistical, compilation and analysis purposes;

• the processing is carried out by political parties, or candidates for election to, or holders of, elective political office, in the course of electoral activities for the purpose of compiling data on people’s political opinions and complies with such requirements (if any) as may be prescribed for the purpose of safeguarding the fundamental rights and freedoms of Data Subjects;

• the processing is authorised by regulations that are made by the Minister and are made for reasons of substantial public interest;

• the processing is necessary for the purpose of the assessment, collection or payment of any tax, duty, levy, or other moneys owed or payable to the State and the data has been provided by the Data Subject solely for that purpose; and

• the processing is necessary for the purposes of determining entitlement to or control of, or any other purpose connected with the administration of any benefit, pension, assistance, allowance, supplement or payment under the Social Welfare (Consolidation) Act 1993, or any non-statutory scheme administered by the Minister for Social Protection.

f. Employee Personal Data

The ODPC has published guidance notes in relation to employment issues and while they are not legally enforceable they would be taken into account by the courts when enforcing the DP Acts. These notes are a practical guide as to how the ODPC considers employers can comply with the DP Acts in relation to employee data and cover areas such as access requests and HR, staff monitoring, considerations when vetting prospective employees, biometrics, whistleblowing and transfer of ownership of a business.

While the ODPC accepts that organisations have a legitimate interest to protect their business, reputation, resources and equipment, the monitoring of employees must comply with the transparency requirements of the DP Acts. Any monitoring must be a proportionate response by an employer to the risk he or she faces taking into account the legitimate privacy and other interests of workers. The ODPC recommends that at a very minimum, staff should be aware of what the employer is collecting on them (directly or from other sources). Staff have a right of access to their data under the DP Acts.

The employer is generally able to justify processing non-sensitive employee Personal Data without the need to obtain the employees’ consent. It can do so, for example, if: (i) it is necessary to perform the employment contract; (ii) it is necessary to comply with a legal obligation; (iii) it is necessary to prevent injury or damage to the health of the Data Subject or to prevent serious loss or
damage to the property of the Data Subject; or (iv) because it is in the employer’s legitimate interests and does not unduly prejudice the employee’s right to privacy or other rights. However, these legitimate interests cannot take precedence over the principles of data protection, including the requirement for transparency, fair and lawful processing of data and the need to ensure that any encroachment on an employee’s privacy is fair and proportionate. A worker can always object to processing on the grounds that it is causing or likely to cause substantial damage or distress to an individual.

If the information being processed is sensitive, explicit consent must be obtained, unless certain limited exceptions apply such as: (i) the processing is necessary to perform or exercise any right or obligation imposed by law in connection with their employment; (ii) the processing is necessary for the purpose of or in connection with legal proceedings or to obtain legal advice; or (iii) the processing is necessary to establish exercise or defend legal rights.

5. Consent

a. General
Consent is not defined in the DP Acts. In practice, while consent of the Data Subject to process Personal Data is not mandatory, it is contemplated as a justification for its processing and is often one of the more straightforward ways to justify processing. Written consent is not required and in certain circumstances, it may be implied. In addition, the Data Subject also has the right to withdraw consent at any time.

In July 2011, the Article 29 Working Party issued an opinion paper on the definition of “consent” as used in the Data Protection Directive (95/46/EC) and the E-Privacy Directive.

b. Sensitive Data
If the information being processed is sensitive (relating to race or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, physical or mental health, sexual life or commission or alleged commission of or a prosecution for an offense) and consent is relied upon to justify the processing of sensitive Personal Data, it must be explicit and must be obtained prior to processing, unless certain limited exceptions apply. The ODPC has clarified that explicit consent means clear, unambiguous and freely given.

c. Minors
The DP Acts do not specify a minimum age at which a child can provide valid consent to having their Personal Data processed. Where a person is under the age of majority (18), the DP Acts require the Data Controller to make a judgement on whether the young person can appreciate the implications of giving consent. The ODPC has issued useful guidance on the issues concerning the age of consent.
Specifically in relation to the right of access to health data, the guidance recommends that the general practitioner use professional judgement on whether the entitlement to access should be exercisable by (i) the individual alone, (ii) a parent or guardian alone, or (iii) both. In making a decision, there is suggestion that particular regard should be had to the maturity of the young person concerned and his or her best interests.

According to the ODPC, where marketing to young people is involved, a person under 18 could be expected to understand the implications of giving consent in suitable cases. It should be considered whether someone under 18 could be expected to understand the implications of giving consent to processing of their Personal Data in order to avail of a particular product or service. Otherwise, the consent of a parent or guardian should be obtained and suitable authentication measures adopted to make sure that such consent is genuine.

d. Employee Consent

The guidance of the Article 29 Working Party sets out the view that consent is not particularly easy to achieve and that the other justifications (see Section 4(f)) should always be considered in preference to consent. The ODPC issued some guidance in respect of consent and the obtaining of medical data in the employment context. An employer would not normally have a legitimate interest in knowing the precise nature of an illness and would therefore be at risk of breaching the DP Acts if they sought such information. The consent of the employee may not allow the disclosure of such information to an employer as there is a doubt as to whether such consent could be considered to be freely given in such circumstances.

e. Online/Electronic Consent

Electronic consent will suffice if appropriate safeguards are taken to ensure a Data Subject is aware of the Data Controller’s data processing notice and has granted consent on that basis (e.g., inclusion of a hyperlink directly above a consent button) and to prevent consent by mistake (e.g., a double click acceptance process). The Data Controller should be able to evidence that such safeguards have been put in place (e.g., the Data Controller should be able to demonstrate that the user was provided with sufficient notice and that consent was informed and voluntary).

6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to contact the privacy officer or person accountable for the organization’s policies and
practices; how to make an inquiry or file a complaint; how to access and/or correct the Data Subject’s Personal Data; and the means of transmission of the Personal Data.

7. Processing Rules
An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements
An organization that collects and processes Personal Data is required to register with the local data authority.

10. Data Protection Officers
In Ireland, there is no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers
Transfers of Personal Data from Ireland to EEA Member States are generally permitted without the need for further approval. Transfers are also permitted to Canada (for certain types of Personal Data), Argentina, Guernsey, the Isle of Man, Jersey, the Faroe Islands, Andorra, Israel, Switzerland, New Zealand and Uruguay, which are the subject of the European Commission’s findings of adequacy (subject to the fulfilment of certain preconditions) in relation to their data protection laws. Transfer to the US is permitted where the recipient has signed up to the US Department of Commerce’s Safe Harbour Privacy Principles. Any US organisation that is subject to the jurisdiction of the Federal Trade Commission (FTC) may participate in Safe Harbour.

Subject to the specific authorizations mentioned above, Personal Data may not be transferred to countries outside the EEA unless the destination country provides adequate protection of the Personal Data. Exceptions to this general prohibition are, however, expressly contemplated under the DP Acts, including where:
• the transfer of Personal Data is required or authorised by law;
• the Data Subject has consented to the transfer;
• the transfer is necessary to perform a contract with the Data Subject, or to take steps at his request with a view to entering into a contract with him;
• the transfer is necessary for the conclusion or performance of a contract entered into between the Data Controller and third parties in the interests of, or at the request of, the Data Subject;
• the transfer is necessary for reasons of substantial public interest;
• the transfer is necessary for obtaining legal advice or in connection with legal proceedings;
• the transfer is necessary to prevent injury or other damage to the data subject’s health, or to prevent serious damage to his or her property, or to protect his or her vital interest in some other way- provided that it is not possible to inform the data subject, or to obtain his or her consent, without harming his or her vital interests;
• the Personal Data to be transferred are an extract from a statutory public register; or
• the transfer has been specifically authorized by the ODPC where the Data Controller can point to adequate data protection safeguards, such as approved contractual provisions.

The adoption of model contractual clauses approved by the European Commission will also provide an adequate level of protection to justify the transfer. (Note that the Data Controller must in any event justify all of its data processing under the DP Acts; justification of any transfers is an additional compliance requirement.) Unlike many other EU Member States, if a transfer contract is used it will not need to be filed or approved by the ODPC, whether before or after any transfers take place. However, it is important to note that Data Controllers which do not have the requisite contracts in place, and which cannot point to alternative data protection safeguards, may be subject to enforcement proceedings under the DP Acts.

Where multinational organizations are transferring personal information outside the EEA, but within their group of companies, they may also adopt Binding Corporate Rules (BCR) as a means of justifying such intra-group transfers. BCR provide adequate safeguards for the protection of privacy with regard to all transfers of Personal Data protected under European law. Acceptable BCR may include intra-group agreements, policies or procedures, and special arrangements among the group of companies that afford the requisite protection.
The ODPC, along with twenty other DPAs across the EEA have agreed to mutually recognise BCR approved by one of these 21 DPAs. For BCR to enable the transfer of personal information freely within a corporate group, they must be approved by at least one DPA that has agreed to mutually recognise BCR applications, and by any remaining DPAs in EEA countries from which the organization transfers Personal Data and which have not agreed to mutual recognition of BCR applications. The Article 29 Working Party has adopted a model checklist and table setting out the required contents of an application to a data protection authority for approval of proposed BCRs.

In January 2012 the ODPC approved Intel Corporation’s BCRs in conjunction with other EU DPAs. The ODPC highlighted how BCR are a valuable tool for entities to embed privacy principles into their business practices and to comply with EU data protection requirements.

12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors. In case of an occurrence of data breach, the outsourcing organization may be held liable together with the third party provider.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
Under the Privacy Regulations, “publicly available communications services” providers (such as telecommunications companies and ISPs) are required to report all incidents in which Personal Data have been put at risk as soon as the Data Controller becomes aware of the incident, except when the full extent and consequences of the incident have been reported without delay directly to the affected Data Subject(s) and it affects no more than 100 Data Subjects and it does not include Sensitive Personal Data or Personal Data of a financial
nature. The ODPC has the ability to audit relevant organizations to assess their compliance with these guidelines and instructions.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions, class actions, and/or a criminal prosecution.

16. Accountability

There is no existing law in Ireland that requires organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. It is also not a requirement to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

17. Whistle-blower hotline

The general filing requirement under the DP Acts applies, and any whistle-blower hotline will constitute one of the Data Controller’s data processing activities in Ireland. That must be covered in its filing (i.e., registration) with the ODPC. The employees should also be informed (in a written policy typically) as to how the data will be processed as part of the hotline procedure.

The ODPC has issued specific guidance in respect of whistleblowing and how to ensure compliance when Personal Data are involved. A best practice approach for an organisation introducing a whistle-blowing scheme is to arrange, where possible, that the data produced from such a scheme refer to issues as opposed to individuals.

18. E-discovery

When implementing an e-discovery system, an organization may be required to obtain the consent of employees if the collection of Personal Data is involved, and advise employees of the implementation of said system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace.

20. Cookies

Organisations may no longer simply provide website users with the opportunity to “opt-out” of the use of cookies, but are now required to obtain the consent of the user to the organisation’s storage of cookies on their device. The Privacy Regulations prohibit the use of an electronic communications network to store information or gain access to information already stored in the terminal equipment of a subscriber or user unless the individual (i) has been given clear and comprehensive information about why
this is being done and (ii) has given consent. Information that is necessary to facilitate the transmission of a communication, or information that is strictly necessary to provide an information society service explicitly requested by the user, is not subject to this requirement. The ODPC issued guidance setting out that in order to meet the legal requirements such settings would require, as a minimum, clear communication to the user as to what they are being asked to consent to in terms of cookies usage and a means of giving or refusing consent to any information being stored or retrieved. It is particularly important that the requirements are met where third party or tracking cookies are involved. Unlike other jurisdictions, there is no formal compliance grace period in Ireland. In December 2012 the ODPC issued correspondence to 80 Irish companies requesting information on how they are complying with the revised rules for cookies, providing 21 days to outline the steps that have been taken to ensure compliance. The ODPC made specific reference to its powers of enforcement in the event of non-compliance.

In December 2013, the ODPC issued updated guidance on the use of cookies. In respect of cookie usage, the ODPC indicated that they would be satisfied with a prominent notice on the homepage of a website informing users about the website’s use of cookies with a link through to a cookie statement containing information sufficient to allow users to make informed choices, together with an option to manage and disable the cookies. From a practical perspective they set out certain minimum requirements for website operators to adhere to as follows:

1. Consent - consent of the user must be captured and may be obtained explicitly through the use of an opt-in check box or may be obtained by implication.

2. Notification - consent should be sought as part of a prominent notification displayed on entry to a website containing a link to a cookie statement which should outline in further detail how the website makes use of cookies.

3. Cookies Statement - this statement should contain clear and comprehensive information on the types of cookies, how cookies are used and details on how to remove them.

4. Third Party Cookies - it is not sufficient to simply refer a user to third party websites. The cookie statement should ideally contain information as to the type of cookies, their name, a description of their purpose, their expiry dates and link to advertising networks’ opt-out mechanisms for third party cookies.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.
Israel

Nurit Dagan
Tel Aviv
Tel: +9722 3 692 7424
dagan@hfn.co.il
1. Recent Privacy Development

The Protection of Privacy Law, 1981 (the “Privacy Law”) regulates the issue of protection of privacy in general, and the matter of protection of privacy in computer databases in particular. The Registrar of Databases (the “Registrar”), which is part of the Israeli Law Information and Technology Authority (“ILITA”), is responsible for the enforcement of the Privacy Law. In accordance with the Registrar’s role, the Registrar has issued from time to time various guidelines which set out ILITA’s interpretation of the Privacy Law and operative instructions and also various recommendations for the general public.

In this regard, we set out in brief some of the principles contained in the guidelines and recommendations issued by ILITA:

i) ILITA published a statement of opinion with respect to the use of biometric attendance control system in the workplace. Under such statement, an employer must: (a) first justify the selection in a mean which infringes privacy, in light of other alternatives which may cause less harm to the privacy and if such justification exists – use such mean in a proportional manner; (b) Refrain as much as possible from storing biometric information in a database (the storage of such information in “smart keys” is advisable); (c) In the event where there is no other alternative but to store biometric information in a database – employ strict data security measures. The legal status of the abovementioned statement is not clear but it indicates how the Registrar interprets the use of biometric attendance systems in the workplace, in light of the Law.

ii) Protection of privacy on the internet ILITA has published recommendations addressed to the general public with respect to using the internet. Such recommendations are intended to raise awareness and provide general tools for coping with the disclosure of personal information on social networks, security risks relating to one’s personal computer, the use of smart phones and downloading applications, tracking activities on the internet, and internet scams.

iii) Guideline No 2-2012, dated February 28, 2012, titled: The Application of the Provisions of the Protection of Privacy Laws on Processes for Screening Applicants for Employment Purposes and the Activities of Employee Screening Centers. This guideline sets out various requirements. For instance, it establishes the requirement to register a database with respect to the information collected during the employee screening process, access rights with respect to such a database, limitations on the uses of the database, the requirement to receive the applicant’s consent to any use of the information, the requirement that the use be subject to general criteria determined by labor law and relevant case law, the requirement that use of the personal information be proportionate and reasonable, the requirement that access rights with
respect to the screening information (including test results) be granted, and the obligation to delete the information or render it anonymous when it is no longer necessary for its applicable purpose.

This guideline has been scrutinized by many screening centers and by the Organization of Psychologists. These organizations have filed petitions with courts against the Registrar and this guideline. During 2013, such petitions were settled and ILITA published an update to the guideline. This update provides, among other things, that access rights granted to the applicant will not include access to certain types of data including: (i) details relating to the potential employer, (ii) specific characterizations of the job, and (iii) analysis of the suitability of the applicant and his/her qualities and personality to the job specifications based on the details detailed in (i) and (ii) above.

iv) Guideline No 4-2012, dated October 21, 2012, titled: The Use of Security and Surveillance Cameras and the Use of Databases Containing Pictures Taken by Those Surveillance Cameras. Under this guideline, the Registrar addresses the application of the Privacy Law with respect to the use of Surveillance Cameras in public areas.

The guideline provides guidance with respect to using Surveillance Cameras and choosing the specific location of such Cameras, the coverage they provide and their specific functionalities. The guideline also states that the public must be informed as to the use of the Surveillance Camera, including by way of placing clear and readable signs and the contents of such warning signs (including, for example, the name of the organization that installed the Camera, the purpose for which it was installed, contact details, etc.). The guideline also sets out instructions with respect to the period of retention of the pictures and their deletion, the rights of inspection of the pictures by those who have been captured on the cameras, various security requirements with respect to the database of pictures, and limitations on the uses of the database.

v) Guideline No 3-2012, dated July 29, 2012, titled: The Application of the Privacy Law on Databases Owned by Private Agencies for Placing of Foreign Employees in the Nursing Field. The purpose of this guideline is to protect the privacy of people who require the services of foreign workers in the nursing field, as these people are usually among the weaker and more vulnerable persons in the general population. The guideline sets out the requirements of the applicable private agencies with respect to: registering databases, receiving applicable consents, the uses and transfer of the personal data, use of data for direct marketing, data security, and conditions of retaining data upon the termination of the services.
vi) Guideline No 2-2012, dated June 10, 2012, titled: *Use of Outsourcing Services for Processing of Personal Data*. This guideline refers to any outsourcing to third parties for the processing of personal data from an Israeli Database.

vii) Guideline No 1-2012, dated February 27, 2012, titled: *The Application of the Provisions of the Protection of Privacy Law on Databases of Public Transportation Operators using “Smart Cards”*. Smart Cards are electronic tickets used for most means of public transportation. They are issued in accordance with certain applicable transportation legislation. This guideline refers to the information collected by the public transportation operators for the purpose of issuing the Smart Cards and through the use of the Smart Cards by passengers. The guideline refers to matters such as: the registration of applicable databases and data security, receipt of informed consents from the passengers to the collection, processing and transfer of the information, and permitted uses of the information.

viii) Guideline No 1-2011, dated September 20, 2011, titled: *Prohibition on the Use of Information Regarding Attachments Imposed on a Third Party*. This Guideline clarifies that a third party (such as a bank, insurance company, etc.) is not permitted to use information regarding the imposition of an attachment on the assets of a debtor that have come to such third party’s knowledge due to an attachment order that was submitted to the third party other than for the purpose stated in the order, without the prior informed consent of the debtor.

2. Emerging Privacy Issues and Trends

Protection of privacy is a developing area in Israel, and it has become more and more predominant, both due to the technological developments which create new risks to privacy (such as social networks, e-commerce, etc.) and the active role taken by ILITA and the Registrar including by increasing the enforcement of the Privacy Law and by raising the public's awareness to privacy matters. During 2013 the head of ILITA was changed and it is still too early to assess the effects of such change on trends in the field.

Some examples of enforcement actions that were taken by the Registrar are published on ILITA’s website, and they include:

i) Imposing administrative fines on companies that used or transferred information from their databases for purposes other than those for which the databases were established.

ii) Imposing an administrative fine for engaging in direct marketing activities in contravention of the requirements of the Privacy Law.
In addition, the Registrar has issued many guidelines in which the Registrar sets out the authority’s interpretation of the Privacy Law with respect to various privacy-related fields. Details of some of the guidelines can be found in Section 1 above.

Furthermore, there are also draft laws and guidelines which to date have still not been enacted or approved. These legal developments demonstrate a focus on strengthening the powers of the Registrar, ensuring the security of databases, and developing privacy awareness in various fields. We have set out below, in brief, some principles set out in such draft legislation and guidelines. It should be noted that currently, the draft legislation and guidelines indicated below are at the very early stages of the enactment or approval process, as applicable, and accordingly it is unclear whether or when they will be enacted or approved, and what their final versions look like.

• In 2013, ILITA updated its forms for registration of databases which are required to be registered under the Privacy Law and for updating registration details. The new and amended application forms are more comprehensive and require the applicant (i.e. the owner of the database) to provide more detailed information than was previously required, such as the sources of the data, information concerning third parties to whom information is transferred, database’s infrastructure, etc.

• On December 9, 2014, 26 Data Protection Authorities worldwide (Israel among them) issued an open letter to operators of app marketplaces (Apple among them), urging them to require each app to provide specific and direct links to privacy policies applicable for apps that collect personal information.

• In October 2013, a non-governmental draft bill initiated by a few members of Parliament was issued, entitled: the Draft Bill Protection of Privacy Law (Amendment- Report on Security Breach in a Database), 2013. The purpose of this draft bill is to require the owner or holder of a database to report cases of penetration of their databases to data subjects and to the Registrar, and in addition, to authorize the Registrar to impose fines in this regard.

It should be noted that currently, this draft bill is at the very early stages of its enactment process and accordingly it is unclear whether and when it will be enacted, and what its final version looks like.

• ILITA published a draft Directive regarding the interpretation and implementation of the Privacy Law provisions relating to direct marketing and direct marketing services. With respect to consent, the Directive states that generally consent for direct marketing and direct marketing services is an opt-out consent, unless the inclusion of the data subject in the database was by way of breach of the Privacy Law. However, the draft Directive further states that the use of information relating to a data
subject, which has been obtained during a relationship between a client and a service provider to which a standard contract (a contract which has been pre-determined by one party in order for it to be used in several agreements between that party and an undetermined and unspecified number of other parties) applies, requires an opt-in consent (except when the service provider wishes to refer to the client offers for services or products which have a direct line to the main service provided by the service provider). The draft Directive has only been published for the public’s comments. Accordingly, the final contents of the Directive as well as the date in which it will come into force, if at all, are unclear at this stage in time.

• In 2013, ILITA published a draft guideline titled: Prohibition on Use by Banks of Information on Restricted Accounts after the Termination of the Restriction Period. This draft guideline would, if implemented, limit the bank’s ability to use information regarding a restricted account in the event that the owner of the account was not the bank’s client during the restriction period. The draft guideline also outlines certain circumstances in which the banks should delete all information regarding restrictions on accounts.

• In November 2011, the government published a draft bill titled: Draft Bill Protection of Privacy Law (Amendment No. 12) (Enforcement Powers), 2011 (the “Draft Enforcement Powers Bill”), as part of its efforts to improve the supervisory and enforcement powers of the Registrar. The Draft Enforcement Powers Bill would enable the Registrar to, among other things: issue security orders with respect to security breaches, penetrating computers, requesting the court to issue various orders, performing investigations, seizing relevant documents and other materials, conducting searches, and imposing various monetary fines. The Draft Enforcement Powers Bill proposes establishing an alternative administrative enforcement mechanism that could be used in parallel with the current enforcement mechanism under the Penal Law 1977.

• In August 2012, an initial draft of an amendment to the Protection of Privacy Law was issued for the public’s comments, titled Reducing Registration Requirements and Determining Obligations to Maintain Management and Work Procedures and their Documentation, 2012. The purpose of this draft bill is to loosen the requirement to register databases and to place more emphasis on improving compliance with the provisions of the Privacy Law by establishing internal procedures and enforcement of the supervisory authorities of the Registrar.

• In June 2012, ILITA published draft regulations titled: Protection of Privacy Regulations (Data Security), 2012. The purpose of these regulations is to specify and determine the principles relating to data security according to different types of databases. These regulations
refer, inter alia, to appointing a data security officer and setting out such
officer’s obligations, an obligation to have a security policy and its
contents, a requirement to conduct a risk survey, physical security
requirements, access rights to the database, documentation and periodic
audits, documenting security events, use of portable devices, security of
data systems and networks, outsourcing data processing, backup and
recoveries, and the authorities of the Registrar in this regard.

- In April 2012, ILITA issued a draft guide entitled: Handbook for Employers
  and Employees on the Protection of Personal Information at the
  Workplace, for the public’s comments. The draft handbook covers various
issues including employee consent limitations and requirements, uses of
information, confidentiality and data security, processing of employees’
personal information during the entire period of the relationship between
the parties (including with respect to applicants, employees and former
employees), and monitoring of employees’ use of various technological
means at the workplace.

3. Law Applicable

In general, the Israeli legislation with respect to privacy issues is governed by
The Basic Law: Human Dignity and Liberty (the "Basic Law") (as Israel does
not have a written Constitution, the Supreme Court of Israel has conferred
constitutional status on such Basic Laws), and the Privacy Law.

Whilst the Basic Law sets out in general terms the fundamental rights of any
person to privacy and to intimacy and further protects in general the privacy
and secrecy of a person’s communications, the Privacy Law and the
subsequent regulations set out in detail provisions for the protection of
personal information (note that the Privacy Law refers to protection of privacy
and of personal information of individuals only and not of entities). These
include a number of substantive issues concerning, inter alia, the processing,
collecting, transferring and maintaining of such information.

Below is a list of the regulations and orders which have been enacted under
or in connection with the Privacy Law:

(i) Protection of Privacy Regulations (Conditions for Viewing Information
    and Procedural Rules for Appealing Against A Refusal to Allow Viewing)
    1981. These regulations establish the procedure for submitting an
    application for viewing information and the viewing process. In addition,
    these regulations set out the reasons according to which an owner of a
    database may reject the application and how to appeal against such
    rejection.

(ii) Protection of Privacy Regulations (Conditions for Holding and Maintaining
    Information and Procedures for Transfer of Information Between Public
    Bodies) 1986. These regulations include general provisions with respect
    to the management of Databases; procedures for the transfer of
information between public bodies; and rules for the management and use of databases that include restricted information.

(iii) **Protection of Privacy Regulations (Designation of Databases That Include Information that May Not be Disclosed) 1987.** These regulations specify databases of particular bodies that may not be disclosed due to national security issues.

(iv) **Protection of Privacy Regulations (Fees), 2000.** These regulations establish the amounts of the registration fees and annual fees with respect to the registered databases.

(v) **Protection of Privacy Regulations (Transfer of Information to Databases Outside the Borders of Israel) 2001.** These regulations establish restrictions and conditions for the transfer of information from an Israeli database to a recipient outside of Israel.

(vi) **Administrative Offences Regulations (Administrative Fine – Protection of Privacy) 2004.** These regulations determine the amount of the administrative fines which can be imposed in the event of any violation of specific provisions of the Privacy Law.

(vii) **Protection of Privacy Order (Designation of Public Bodies) 1986.** These regulations set out a list of bodies to be considered as public bodies under the Privacy Law (in addition to the public bodies listed in the Privacy Law).

(viii) **Protection of Privacy Order (Designation of Investigation Authority) 1998.** These regulations set out specific authorities that have investigatory powers and the databases of which are therefore not subject to viewing rights of data subjects.

(ix) **Protection of Privacy Order (Establishment of Supervision Unit) 1999.** These Regulations establish a supervisory unit for supervision of databases, their registration and data security.

4. Key Privacy Concepts

a. **Personal Data**

The Privacy Law handles both general matters of privacy as well as the protection of privacy in computerized databases.

The first chapter of the Privacy Law regulates the infringement of privacy in general and establishes eleven occurrences which constitute an infringement of privacy, if done without the consent of the data subject:

(i) spying on or trailing a person in a manner likely to harass him, or any other harassment;

(ii) listening (wiretapping) in a manner prohibited under any law;
(iii) photographing a person while he is in a private domain;

(iv) publicizing a person’s photograph under circumstances in which the publication is likely to humiliate the person (there is an additional specific provision with respect to publicizing a photograph of injured persons during the occurrence of the injury or in proximity thereto in an identifiable manner which might humiliate them, excluding certain live broadcasting; in addition, under certain circumstances publicizing a picture of a deceased in a manner which could identify him/her will also be deemed to a breach of privacy);

(v) publication of a victim’s photograph, shot during the time of injury or immediately thereafter, in a manner where he is identifiable and under circumstances by which the publication thereof is likely to embarrass him, except for the immediate publication of a photograph, without delays between the moment of photographing and the moment of actual transmission of broadcast, which is reasonable under the circumstances; for this purpose, “victim” – a person who suffered physical or mental injury due to a sudden event and the injury thereof is noticeable.

(vi) copying or using, without permission from the addressee or the writer, the contents of a letter or of any other writing not intended for publication, unless the writing is of historical value or fifteen years have passed since the time when it was written (this provision refers also to electronic messages);

(vii) using a person’s name, appellation, picture or voice for profit;

(viii) infringing an obligation of secrecy laid down by law in respect of a person’s private affairs;

(ix) infringing an obligation of secrecy laid down by explicit or implicit agreement in respect of a person’s private affairs;

(x) using, or passing on to another, information on a person’s private affairs, other than for the purpose for which it was given;

(xi) publicizing or passing on anything that was obtained by way of an infringement of privacy under paragraphs (i) to (viii) or (x) above; or

(xii) publicizing any matter that relates to a person’s intimate life, state of health or conduct in the private domain.

The second chapter of the Privacy Law regulates the protection of privacy in databases. According to the Privacy Law, the definition of “Database” is “a collection of information, maintained by magnetic or optical means and intended for computer processing”, subject to the following exclusions: a collection of information that includes only names, addresses and means of communicating, which by themselves do not create any characteristics that infringe the privacy of individuals whose names are included on it, on the
condition that neither the owner of the collection, nor a body corporate under its control, owns an additional collection.

Furthermore, “Information” is defined as “information about an individual’s personality, personal status, intimate affairs, health condition, financial condition, professional qualifications, opinions and beliefs”.

The Privacy Law further defines “Sensitive Information” as “information about an individual’s personality, intimate affairs, health condition, financial condition, opinions and beliefs”.

When a database includes Sensitive Information, this is one of the conditions under the Privacy Law for the registration of such database.

It should be noted that according to Israeli case law, the definitions mentioned above of “Information” and “Sensitive Information” should be interpreted broadly. Accordingly, for example, a person’s identity number and date of birth might be considered Sensitive Information which requires the registration of a database. Whether information is sensitive depends on the specific circumstances including the aggregate scope of information maintained about the data subject.

b. Data Processing

We note that the Privacy Law does not define the term “Data Processing”. However, there is a definition of the term “Use” as including: “disclosure, transfer and delivery”.

Furthermore, according to the Privacy Law, no person shall use Information in a database that must be registered under the Privacy Law for purposes other than those for which the database was established.

In addition, under the Privacy Law, any request to a person for information, with the intention of maintaining and using it in a database, must be accompanied by a notice that indicates, inter alia, the purpose for which the information is requested, to whom the information is to be provided, and for what purpose. The database may not be used in a different manner than what was indicated in the notice without requesting an additional consent of the data subject.

c. Processing by Data Controllers

The Privacy Law applies to any person or entity that either owns or holds a database. In certain cases, specific provisions of the Law apply to their employees and to the manager of the database (such as with respect to confidentiality obligations).
d. Jurisdiction/Territoriality

In general, the Privacy Law, as part of the Israeli civil legislation, has territorial application. Accordingly, the Privacy Law will apply to offenses which have been committed in Israel in respect of violations of the applicable provisions of the Privacy Law.

However, it should be noted that there is one decision rendered by the District Court relating to the area of gambling, according to which operating an online gaming website was regarded as a domestic offense, even if the owner of the website is a foreign company, in the event that the website specifically addresses Israelis (such as translation of the website into Hebrew, the marketing of activities in Israel, etc.). The Court determined that the offence itself will have been “completed” in Israel when the Israeli gambler gambled through the website (by clicking the computer mouse) and accordingly, participation in the proposed activity of the gambling organization. The principles of this case could be applied to the Privacy Law as well, mutatis mutandis.

e. Sensitive Personal Data

According to the Privacy Law, “Sensitive Information” is defined as one of the following:

(1) Information about an individual’s personality, intimate affairs, health condition, financial condition, opinions and beliefs.

(2) Information which the Minister of Justice, by order (with the approval of the Israeli Parliament’s Constitution, Law and Justice Committee) has referred to as sensitive information.

As we have noted above, according to the Privacy Law, when a database includes sensitive information, it must be registered. It should be noted that the term sensitive information is interpreted broadly according to Israeli case law.

f. Employee Personal Data

The Privacy Law also applies to personal data concerning employees. Inevitably, employers are required to process both personal information as well as sensitive information regarding their employees (and potential employees). With respect to employees, according to case law, due to the nature of the relationship between the employer and the employee (i.e., the employee being in a relative position of weakness vis-a-vis the employer, with the result that the employee may be overzealous in his or her willingness to grant the employer broad consents over a wide range of information), the court will also carry out a review as to whether the employer’s actions, including the collection of any employee personal information, obtaining employee consents and the uses of the information, were undertaken in good
faith and if they were proportional and relevant to the employment relationship.

5. Consent Requirements

a. General

Consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data. Consent must be informed, which means that the person should receive sufficient information with respect to the matter in order to be able to reach a decision whether or not to provide the Personal Data. In general, such consent could either be explicit or implicit.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the data subject, and sensitivity of the personal data.

b. Sensitive Data

The same general rules above apply with respect to Sensitive Data. However, in general, the scrutiny of the informed consent is likely to be more stringent when it comes to Sensitive Data.

c. Minors

In general, the Privacy Law does not include any specific reference to minors and minors’ consent and accordingly the consent requirements detailed above would apply to them as well, subject to the provisions of the Legal Capacity and Guardianship Law 1962 (the “Capacity Law”) which governs matters relating to minors.

Under the Capacity Law, the legal acts of a minor (i.e. a person under the age of 18) may be cancelled if performed without the consent of a parent/guardian. However, legal acts of a kind that minors of his/her age are accustomed to perform, or legal acts performed with a person who did not or could not reasonably be expected to know that the minor is a minor, may not be cancelled unless they involve material damage to the minor or his/her property. This general rule would be applicable to any consent provided by a minor for the purpose of compliance with the provisions of the Privacy Law.

It should be noted that in December 2010, ILITA issued certain draft general principles (which are, as of this date, non-official and non-binding) which refer to the collection of information from minors over the internet. According to the draft principles, the collection of information will require, under certain circumstances, the consent of a parent/guardian, regardless of the qualifications set out under the Capacity Law, as the consent of a minor in this aspect should be dependent on the minor’s ability to understand the notice provided to the minor regarding the collection of information from such minor.
Accordingly, ILITA recommends, *inter alia*: (i) restricting the collection and publication of information from minors under the age of 14, without the consent of a parent/guardian and restricting the collection and publication of sensitive information from minors under the age of 18, without the consent of a parent/guardian; (ii) requiring bodies who collect information from minors to set out and publish a defined and clear privacy policy; (iii) restricting the transfer of or trade in minor’s data to or with third parties; (iv) requiring bodies who collect information from minors to comply with certain security measures; and (v) erasing information of minors which is no longer needed or at the request of the minor’s parent or guardian.

d. Employee Consent

Under Israeli case law, an implicit consent is not sufficient with respect to employees and the employee is required to give his/her explicit consent (usually in writing) with respect to his/her waiver of his/her right to privacy.

In addition, the employee’s consent should be examined in light of the following conditions:

- **condition of legitimacy** – the violation of the privacy right must be limited to essential business purposes;
- **condition of proportionality** – the employer should examine and select the means which are the least harmful to the employees’ privacy;
- **principle of proximity to the purpose** – the collection of information is limited only to what is necessary in order to achieve the initial purpose for which the information was collected in the first place.

Moreover, the general policy which is applicable in the workplace, with respect to privacy matters, should be approved by the employee.

e. Online/Electronic Consent

Electronic consent is permissible and can be effective in Israel if it is properly structured and evidenced.

6. Information/Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; and where the Personal Data is to be transferred.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/
anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. Registration/Notification Requirements

Organizations that collect and process Personal Data may be required to register, file or notify the local data authority.

10. Data Protection Officers

Organizations may be required to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

Specific regulations have been enacted with respect to the transfer of data from a database in Israel outside of Israel, entitled: The Protection of Privacy Regulations (the Transfer of Information to a Database outside the State Borders), 2001 (the “Transfer Regulations”). The Transfer Regulations impose restrictions in addition to all other restrictions on transfer of information which appear in the Privacy Law, as follows:

(i) The Transfer Regulations prohibit the transfer of information from a database in Israel to a database located abroad, unless the receiving country ensures a level of protection of Information that equals or exceeds the level of protection provided for under Israeli law.

(ii) In addition, the Transfer Regulations lay down several conditions which enable the transfer of information from a database in Israel to a database abroad, even when the laws of the country in which the data will be received provide a level of protection which falls below that which is provided under Israeli law, subject to compliance with any one of the following conditions:

- receipt of a consent to the transfer of the information from the person who is the subject of the information;
- it is not possible to obtain the consent of the person who is the subject of the information, but its transfer is absolutely necessary in order to protect his/her health or the integrity of his/her physical body;
• the information is being transferred to a corporation under the control (i.e. the ability to direct the activities of an entity) of the owner of the Israeli database and it has ensured the protection of privacy following the transfer;

• the information is being transferred to someone who has undertaken in an agreement, with the owner of the Israeli database, to fulfill the conditions laid down in Israel for the maintenance and use of the information, mutatis mutandis;

• the information was made public by the lawful authority, or it was made available for inspection by the public under lawful authority;

• transferring the information is essential for the protection of public welfare and security;

• transferring the information is required by Israeli law; or

• the information is being transferred to a database in a country in which any one of the following conditions exist: (a) it is a party to the European Convention for the Protection of Individuals in connection with automatic processing of Sensitive Information; (b) it receives information from member states in the European Union, under the same conditions of receipt; (c) the Registrar has notified with respect to the destination country, in a notification which has been published in the Official Gazette, that there exists in such country a designated authority to protect privacy, after it has reached an arrangement for cooperation with such authority (to date the Registrar has not issued any such notification).

In addition to the completion of the above conditions (either under subsection i) or ii)), the Transfer Regulations state that the owner of the database must ensure (by way of a written obligation from the recipient of the information) that the recipient shall take action to ensure the privacy of the person to whom the information relates, and that the recipient undertakes that the information shall not be transferred to any person other than the recipient, whether or not such person/entity be in the same country.

12. Security Requirements
Organizations are required to take steps to: ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.
13. Special Rules for Outsourcing of Data Processing to Third Parties

ILITA has issued guidelines entitled “Use of Outsourcing Services for Processing of Personal Data”, which refer to any outsourcing to a third party of the processing of personal data from an Israeli database. These guidelines require that an agreement be entered into with the service provider which should include various matters. In addition, prior to entering into any agreement for the processing of personal data, such outsourcing should be reviewed carefully in order to ascertain its necessity and compliance with data protection laws. Under these guidelines, the following matters, *inter alia*, should be covered by the agreement with respect to outsourcing services:

- The agreement should establish the purpose of the transfer of information and limitations on its uses and transfer.
- Upon the termination of the agreement, the service provider should sign an affidavit confirming that the service provider has either returned the personal information or destroyed it.
- The service provider should store the information separately from the information of its other clients or its other commercial activities.
- Access and correction rights of data subjects are to be determined in the agreement (including with respect to timing and costs).
- The service provider should hold regular guidance sessions to its employees and they should also sign NDAs.
- The parties should each appoint a contact person with respect to the agreement.
- The service provider should provide on-going reports with respect to the performance of the agreement and there should be extensive supervisory rights of the service provider’s activities (including audit and inspection rights).
- The agreement should define a complete binding security document which should include reference to specific matters, such as, physical security, applicable security measures according to the sensitivity of the data, separation of the database from the service provider’s other databases, policies with respect to: storage means, management of the database, access rights, etc. As an alternative to the above security document, the service provider could undertake as part of the agreement to comply with the provisions of ISO/IEC 27001.
- The service provider should appoint a security officer (provided that the service provider maintains databases of more than five clients for such data processing services).
14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings, and/or private rights of action.

15. Data Security Breach

Under Israeli law, there is no mandatory requirement to provide a notice to any data protection authority or other government agent in the event of a data security breach. Similarly, there is no mandatory legal obligation to provide any notification to the affected individuals of a data security breach.

We would note that there currently is a non-governmental draft bill initiated by a few members of parliament, entitled: Draft Bill Protection of Privacy Law (Amendment- Report on Security Breach in a Database), 2012. Such draft bill requires the owner or holder of a database to report cases of penetration into their databases to Data Subjects and to the Registrar. However, this draft bill is at the very early stages of its enactment process and accordingly it is unclear whether and when it will be enacted and what the final version will look like.

Despite the absence of any mandatory requirement, notification to the affected individuals is something that should be considered in order to reduce any possible damages and exposure under tort and contract law, if in the applicable circumstances, such damages or exposure might exist.

An organization that is involved in a data breach situation may be subject to closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions and/or class actions, or a criminal prosecution.

16. Accountability

Subject to regulatory guidance, organizations may be required to conduct privacy impact assessments prior to implementing new information systems and/or technologies for the processing of Personal Data.

As such, organizations are required to furnish the results of privacy impact assessments to privacy regulators upon request, and to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.

17. Whistle-Blower Hotline

There are no specific laws/rules regarding whistle-blower hotlines in Israel. In general, whistle-blower hotlines may be established in Israel as long as they are in compliance with local laws, e.g., registration might be required in...
connection with the hotline under general privacy laws, depending on the specific circumstances of the matter.

18. E-Discovery

When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of Personal Data is involved. Organizations may be required to advise employees of the implementation of said system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace, and give employees the opportunity to opt-out from the spam-filtering.

20. Cookies

There are no specific laws/rules in Israel that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. As such, consent of Data Subjects may have to be obtained before cookies can be used.

In addition, some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.
Italy

Francesca Gaudino
Milan
Tel: +39 02 76231 452
francesca.gaudino@bakermckenzie.com

Lorenzo de Martinis
Milan
Tel: +39 02 76231-334
lorenzo.de.martinis@bakermckenzie.com
1. Recent Privacy Developments

*Italian privacy authority calls for new security measures for Internet Exchange Points (“Ixp”)*

In the course of a number of inspections carried out during 2014 on Italian Internet eXchange Points located in different cities (for example, in Milan, Rome and Turin), the Italian data protection authority (“Garante”) has focused on issues that have emerged in relation to security, specifically in terms of protection of the communication networks.

As a result, the authority has provided a number of precautions to be adopted, reserving the right to further develop the measures to be adopted in specific cases.

The Garante’s investigation falls within the first stage of the process undertaken by Italian providers of Internet connection centers aimed at ensuring that personal information is properly protected and that applicable technical systems are duly updated and monitored in light of constant technology developments.

The Garante has sent the findings of the report stemming from said investigations to the President of the Council of Ministers for due assessment by subjects in charge of national cybersecurity in consideration of the fact that security of electronic communications is a matter that also involves other institutional stakeholders. As a result, some guidelines for network security have been identified.

Internet eXchange Points basically deal with interconnecting network infrastructure of major national and international telecommunications operators of Internet service providers as well as of major providers of online services and functionalities. IxPs also serve the purpose of hosting the equipment that manage communication networks among almost all Italian public administrations and research centers.

The following are some of the measures requested by the Italian privacy authority: (i) Systems should not be accessed using shared authentication credentials, notably shared identifying codes, so as to identify and track access and use of the relevant systems by a single user; (ii) Tight physical measures must be adopted to control security of places via access controls and surveillance precautions where data is stored and processed, with focus given on infrastructure and data centers that may be easily accessed; (iii) Proper tracking systems must be implemented to analyze the activities performed by technical personnel on relevant equipment. This tracking is aimed at identifying possible anomalies and emergencies, including the duplication of Internet traffic, access of non-authorized electronic instruments to the internal network, and deviation of Internet traffic; (iv) Specific procedures and mechanisms must be set up to perform audit and to generate alerts in order to prevent and detect harmful events occurring in the relevant
systems; (v) In cases where external data centers are used, specific procedures must be adopted in order to make sure that third parties are duly and regularly verified, especially in relation to compliance with data security requirements.

**Cookies**

In January 2015, the Garante published an informative video that explains in an easy and clear manner what cookies are and how online users can express their preferences and defend against cookies.

This initiative follows the enactment of the rules on cookies in Italy.

Article 122 of the Privacy Code (Legislative Decree 196/2003 and following amendments and integrations) states the following on cookies:

1. Storing information, or accessing information that is already stored, in the terminal equipment of a contracting party or user shall only be permitted on condition that the contracting party or user has given his consent after being informed in accordance with the simplified arrangements mentioned in section 13(3). This shall be without prejudice to technical storage or access to stored information where they are aimed exclusively at carrying out the transmission of a communication on an electronic communications network, or insofar as this is strictly necessary to the provider of an information society service that has been explicitly requested by the contracting party or user to provide the said service. In order to determine the simplified arrangements referred to herein, the Garante shall also take account of the proposals put forward by the representative consumer and industry associations involved in order to also ensure that the mechanisms implemented make the contracting party or user actually aware.

2. With a view to giving the consent referred to in paragraph 1 above, specific configurations of software or devices may be used that should be user-friendly as well as unambiguous vis-à-vis the contracting party or user.

2-bis. Subject to the provisions made in paragraph 1 above, it shall be prohibited to use an electronic communications network in order to access information stored in the terminal equipment of a contracting party or user, store information, or monitor the operations performed by the user.”

The Garante provided some implementation guidelines on May 8, 2014 - Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies. In brief, the Garante supports a double-decker approach, in the sense that a first high level privacy statement should be displayed through a pop-up language (e.g., a banner) published on the landing page of a website that provides brief information, to be coupled by a more comprehensive privacy statement that has to be referenced in the short
privacy statement through a link. Consent should be obtained through the initial banner in a simplified form, as required by law, and users shall be given the opportunity to express granular and specific consent in relation to the different types of cookies used by accessing the second, more comprehensive privacy statement.

**e-Health**

Following complaints from persons worried about the protection and confidentiality of their data, the Privacy authority has started an investigation against a hospital located in northern Italy. The audit was completed in January 2015 with a number of recommendations concerning the security measures - e.g., physical, technical and organizational precautions put in place by a data controller as an appropriate defense against possible data misuse and breach.

Specifically, the infringer has been allegedly building an electronic health database without gathering the informed consent of the data subjects. In addition, the system hosting the medical records had no proper access control measures, since records could be viewed by a large number of persons simply using search words like partial names and surnames of patients, dates of birth, or zip codes.

This is in contrast to the applicable provisions issued by the Garante in 2009, which mandated detailed security precautions to protect e-health records, including securing a patient’s prior express consent to store medical information through e-health records. In addition, the patient must be provided with the option to make available only some of said records and he/she must be clearly informed of the persons who may access the records and of the actions that they can carry out on the relevant medical data, prior to giving consent.

The privacy authority has thus ordered that medical records be made available only on a need-to-know basis to the relevant doctors, until patients provide their express and specific consent to the e-health record system.

The order of the privacy authority has been made available for consultation to other entities of the national health service.

2. Emerging Privacy Issues and Trends

**Inspection activities**

For the year 2014, the annual report of the Italian privacy authority reveals that fines that have been imposed reached more than EUR 4 million. The breaches include:

(i) failure to provide appropriate information to the data subjects;

(ii) unlawful data processing;
(iii) breaches of orders and provisions of the Garante; and
(iv) failure to comply with opt-out obligations in relation to marketing activities.

The inspection plan for the year 2014 has focused on both ‘traditional’ and new areas of interest.

Matters that represent a returning focus of attention include:

- big data in the public sector;
- banks;
- direct marketing;
- telephone operators; and
- mobile payment.

The new areas of interest include:

- call centers located in non-EU countries;
- customer and online profiling;
- major hotel chains;
- adoption of new technologies in the workplace;
- e-health and medical Apps;
- social media;
- Internet Exchange Points (IXPs);
- data breaches

As to the last item (data breaches), it should be recalled that as currently drafted, the Privacy Code provides for a duty to warn the Garante and (under some instances) also the data subjects in case of data breaches only for providers of publicly available electronic communications services.

The threshold of fines issued by the Garante in 2014 is about EUR 5 million and the number of inspections carried out amounts to 385 while the number of administrative breaches sanctioned amounts to 577. Lastly, 39 criminal cases have been referred by the Garante to judicial authorities.

It is worth mentioning that the Garante actively joins national and international initiatives with other European data protection authorities and also regulatory authorities in relation to compliance auditing and enforcement activities.
National and international cooperation - the case of cookies

The Italian privacy authority is fairly active in collaborating with other European privacy authorities.

Close collaboration can also be seen in relation to other (non privacy) authorities, international bodies and associations that deal with privacy issues or with issues overlapping with privacy, e.g., consumer protection authorities and international privacy organizations.

The Garante, for example, is part of the Global Privacy Enforcement Network (GPEN), which is an informal network of authorities with enforcement powers that has been established with an aim to ease and foster cooperation among authorities at a cross-border level.

An example of a joint action launched at a European level is the so-called ‘Cookie sweep day’ initiative.

From 15 to 19 September 2014, the Article 29 Working Party launched a coordinated assessment conducted by privacy authorities on the most visited European websites involved in e-commerce and media activities which target European users. The aim of the assessment was to verify compliance of said websites with applicable cookies regulations.

The ultimate goal of the Cookie sweep day was to conduct an assessment in relation to general European requirements of information and consent, while gathering information on a comparative basis of Member States’ practices in relation to cookies, also in light of fostering a certain degree of harmonization. Privacy authorities involved may further make use of the results achieved for enforcement purposes at a national level.

3. Law Applicable

The Data Protection Directive (Directive 95/46/EC), the Directive on Privacy and Electronic Communications (Directive 2000/58/EC), the Directive on Data Retention (Directive 2006/24/EC) and the Cookies Directive (Directive 2009/136/EC) have been implemented by Legislative Decree no. 196 of 30 June 2003, which enacted a code on the protection of Personal Data (the “Code”). The Code is primarily intended to consolidate all pre-existing Italian data protection rules, which were replaced by the Code. Furthermore, the Code provides for additional protections for Data Subjects (defined below) and simplifies the applicable rules. The Code attempts to ensure consistency between privacy rules and other legal provisions applicable to various sectors. The Code combines the provisions of the former basic privacy law and subsequent amendments, regulations, and codes of ethics, as well as the case law precedents of the Italian Data Protection Authority.
The Code is organized into three parts: the first, containing general data protection provisions; the second, containing provisions applicable to specific sectors (e.g., judicial sector; public sector; health care sector; educational sector; processing for historic, scientific and statistical purposes; work and social security issues; banking, financial and insurance sectors; electronic communications; professionals and private detectives; journalism, literary and artistic sectors; direct marketing); and the third, on remedies and sanctions for breach of the Code.

The Code applies to the processing of information relating to “Data Subjects” as outlined below.

4. Key Privacy Concepts

a. Personal Data

The Code applies to the processing of information relating to natural persons (“Data Subject”); legal entities and bodies or associations are within the scope of the Code only for limited purposes. Data is considered “personal” where a person can be identified from that data directly or indirectly by reference to any other information (e.g., through cross-referencing via a personal identification number) (“Personal Data”). The information necessary for the identification can be held by the Data Controller (defined below) processing data or by any other third party. Thus, the definition of Personal Data is significantly broad. In practice, only anonymous data (e.g., data that do not allow identification of the Data Subject, whether directly or indirectly) are not subject to application of the Code.

b. Data Processing

As in the applicable Directive, the term “processing” is extremely broadly defined to mean any operation or set of operations carried out on Personal Data, including the collection, recording, organization, keeping, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure, and destruction of Personal Data. Even mere reading is considered processing of Personal Data. The Code applies to electronic, automated and non-electronic (manual and paper) data processing.

c. Processing by Data Controllers

The Code applies to those who determine the purposes for which and the manner in which any Personal Data is will be processed (“Data Controllers”).

d. Jurisdiction/Territoriality

The Code applies to data processing activities performed by a Data Controller established within Italy, and to data processing activities performed by Data Controllers that are established outside the EEA but that use equipment based in Italy to carry out data processing activities (other than merely for the purpose of transit).
e. Sensitive Personal Data

The Code imposes additional requirements for the processing of sensitive Personal Data – that is, Personal Data relating to racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, and data concerning health or sexual life. Specifically, the processing of sensitive Personal Data is prohibited unless the following conditions are met: the Data Controller provides an information notice drafted pursuant to the Code and obtains the explicit written consent of the Data Subject; limited exceptions apply (see Sections 4(f) and 5(b) below); and the Data Controller has the prior authorization of the Authority. The Authority has issued general authorizations that cover usual business activities. A specific authorization is required when the Data Controller intends to perform a data processing activity that does not fall within the general authorizations issued by the Authority.

f. Employee Personal Data

Employee Personal Data is likely to include sensitive Personal Data (e.g., health- and trade union-related information) and non-sensitive Personal Data. Sensitive Personal Data relating to an employee may be processed provided that the requirements mentioned in Section 4(e) above are met. The employee’s consent is not necessarily limited to the Sensitive Personal data whose processing is necessary to comply with specific obligations and/or tasks laid down by laws, regulations or Community legislation in the employment context, also when they relate to occupational and population hygiene and safety and to social security and assistance purposes. In addition, recent legal reform has introduced a further exemption from the written consent requirement. Written consent is not required for the processing of sensitive data of candidates, when such data are contained in the CV that is sent by candidates. One of the general authorizations issued by the Authority applies to employee sensitive Personal Data. This allows Data Controllers to process an employee’s sensitive Personal Data in certain circumstances and for certain purposes specified in the authorization.

Non-sensitive Personal Data relating to an employee may be processed by a Data Controller in certain circumstances, including where the processing is necessary for the performance of the employment agreement or where the processing is necessary for compliance with a labor law or tax obligation of the employer. A fallback justification for processing both sensitive and non-sensitive Personal Data in the employment context may be available if consent (written, in the case of sensitive Personal Data) is provided by the Data Subject (see Section 5(d), below).

The Authority issued two regulations on the processing of employees’ Personal Data and sensitive Personal Data in November 2006 and March 2007. The regulations impose an obligation on the employer to comply with the principles of transparency and proportionality, so that only data that is strictly necessary for a specified purpose may be processed. Further, the
consent of the employee must be obtained when there is no other legitimate
ground for the processing. Moreover, if the employer provides its employees
with personal computers, access to the Internet and email accounts, the
employer must fulfill certain requirements. For example, the employer should
clearly specify to the employees the conditions and limits of the use of the
company’s information system and relevant resources, and it should also
clarify, among other matters, whether personal use is allowed, the relevant
conditions (e.g., time and duration), and whether and how the employer
intends to perform monitoring activities (including the specific circumstances
and purposes of said monitoring). The employer should also seek approval
from trade unions or the competent labor office.

5. Consent

a. General

Consent of the Data Subject is generally required prior to the collection,
processing and disclosure of Personal Data. Consent by the Data Subject
must always be voluntary, informed, explicit and unambiguous, though it is not
required in certain prescribed circumstances.

Consent can be express or implied, but the appropriate form of consent will
depend on the circumstances, expectations of the Data Subject, and
sensitivity of the Personal Data. When the Data Subject gives consent, it is
understood that such consent only covers the identified purpose(s). Fresh
consent is required for purposes that have not been previously identified and
consented to.

Consent must be in the local language. The Data Subject also has the right to
withdraw consent at any time in given circumstances.

b. Sensitive Data

Sensitive Personal Data is recognized as a special category of Personal Data
and is subject to additional or special consent requirements. Sensitive
Personal Data may only be collected and processed with the express consent
of the Data Subject.

For the processing of sensitive Personal Data, written consent must be
provided – that is, in the form of a handwritten or digital signature of the Data
Subject. Limited exceptions apply (See Section 4(f) above).

c. Minors

A person under the age of 18 cannot give valid consent. A parent or legal
guardian must give consent on behalf of the minor. In general, when the minor
becomes of age it is necessary to obtain confirmation of the consent
previously provided by parents or guardians.
d. Employee Consent
Consent given by an employee to the processing of his or her Personal Data is generally considered valid. The usual business practice and advisable procedure is to have a specific privacy document containing the information notice and consent form, incorporated by reference in the employment agreement. If Personal Data is also to be processed for purposes unrelated to the employment agreement (for example, if Personal Data is disclosed to business partners or other companies that may offer products or services to the employees, or if employees’ Personal Data such as pictures or professional information are published on the company’s intranet), the Authority recommends that these additional purposes be specifically approved by the employees through separate consent.

e. Online/Electronic Consent
Electronic consent is permissible and can be effective in Italy provided that it is properly structured and evidenced. For sensitive Personal Data, however, electronic consent may only be permissible in very limited circumstances.

6. Information/Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; the organization’s privacy practices (which must be provided in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to contact the privacy officer or other person accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; how to access and/or correct the Data Subject’s Personal Data; the duration of the proposed processing; and the means of transmission of the Personal Data.

7. Processing Rules
An organization that processes Personal Data must: limit the use of the Personal Data to those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; anonymize the Personal Data whenever possible; provide the Data Subject the option of using a pseudonym or remaining anonymous whenever possible; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; access the Data Subject’s Personal Data,
subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. Registration/Notification Requirements

Organizations that collect and process Personal Data may be required to register, file or notify the local data authority.

10. Data Protection Officers

There is no such a privacy role under the Code. It is possible to appoint an internal data processor (Responsabile del trattamento) for managing privacy issues within an organization on behalf of the Data Controller. In case of third party service providers processing Personal Data in delivery of relevant services, they must be appointed by the Data Controller as external data processors.

11. International Data Transfers

Transfer of Personal Data between member states of the EEA is generally permitted without the need for formal approval by the Authority. Furthermore, no restrictions apply to the transfer of Personal Data to recipients in countries that have been recognized by the European Commission as granting an adequate level of protection to Data Subjects. This is the case for transfers to Switzerland, the Isle of Man, Guernsey, Argentina, Canada, and US-based companies adhering to the Safe Harbor agreement. In the above referenced cases, the transfer of Personal Data is regulated as a communication of Personal Data, thus relevant requirements apply. Transfers outside the EEA are prohibited where the third country does not ensure an adequate level of protection of Personal Data. Exceptions are as follows:

- the Data Subject has given his or her express consent to the transfer (written consent is required for sensitive Personal Data);
- the transfer is necessary for the performance of obligations resulting from a contract to which the Data Subject is a party, or for gathering information at the Data Subject’s request prior to entering into a contract, or for the conclusion or performance of a contract made in the interest of the Data Subject;
- the transfer is necessary for safeguarding an important public interest;
- the transfer is necessary for carrying out criminal investigations;
- the transfer is necessary to safeguard the life or bodily integrity either of the Data Subject or of a third party, and the Data Subject cannot give his or her consent because of physical or legal incapacity or mental disorder;
• the transfer is carried out in response to a request for access to administrative documents or for information included in a public register, list, act, or document which is publicly available, in compliance with the provisions applying to such subject matter; and

• the transfer is authorized by the Authority on the basis of adequate guarantees for the Data Subject’s rights, as resulting from contractual clauses in a data transfer agreement.

The following specific requirements relate to the use of a data transfer agreement: incorporation (or incorporation by reference) of the European Commission’s model clauses for transfer of data between Data Controllers or towards Data Processors into the data transfer agreement by the data exporter and the importer, so that they are available, upon request, to the Data Subjects to whom the Personal Data relates; a copy of the data transfer agreement must be provided to the Authority upon request of the Authority; the choice made in case of a dispute that is not settled amicably and is submitted to an entity other than either the Authority or a judicial authority must be communicated to the Authority; the Data Subjects must be informed of the transfer and the fact that the data transfer agreement is in place. When the aforementioned conditions are met, no formal approval of the data transfer agreements by the Authority is required.

12. Security Requirements

An organization is required to take steps to: ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and are required to comply with sector specific requirements. Organizations may be held liable together with third party providers in the event of breach by the latter.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints; data authority investigations/audits; data authority orders; administrative fines, penalties or sanctions; seizure of equipment or data; civil actions; class actions; criminal proceedings; and/or private rights of action.
15. Data Security Breach

The Code provides for an obligation of disclosure to Data Subjects and/or the Authority or other authorities in the event of a security breach limited to specific sectors (e.g. telecoms operators). In any case, the Data Controller is liable to compensate not only for monetary but also for moral damages caused by the data processing. Thus, also for companies not subject to a disclosure obligation under the Code, in the event of security breaches organizations that are involved in a data breach situation should: gather information about the breach; assess the potential risk of harm to the Data Subject(s); take steps to mitigate the harm to the impacted Data Subject(s); take steps to contain the breach and to prevent future similar breaches; assist authorities with any investigation relating to the breach; and comply with data authority orders and court orders.

An organization that is involved in a data breach situation may be subject to a suspension of business operations; closure or cancellation of the file, register or database; an administrative fine, penalty or sanction; civil actions and/or class actions; or a criminal prosecution.

16. Accountability

Organizations are required to: conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data; furnish the results of the privacy impact assessments to privacy regulators upon request; and furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Italy as long as they are in compliance with local laws.

18. E-Discovery

Employers should advise employees of the implementation of an e-discovery system, the features and purposes of the said system, and (if applicable) that the use of work tools (e.g., email, Internet) is being monitored and that information such as emails is stored. Employers should also specify the features of the monitoring activities and the consequences of failure by employees to comply with the employer’s guidelines on the correct use of the employer’s electronic equipment and system. An employer should also specifically inform employees whether and to what extent electronic devices and equipment provided by the employer for business purposes may also be used for personal purposes. The above information should be contained in a specific IT policy that the employer provides to its employees, and that is agreed upon with trade unions or the competent labor office, as applicable.
19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to: inform employees of monitoring policies being implemented in the workplace; give employees the opportunity to opt out from the spam-filtering solution; and give employees the opportunity to review the isolated emails designated as spam.

20. Cookies

The use of cookies must comply with data privacy laws. As such, consent of Data Subjects must be obtained before cookies can be used and deployed.

Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. Consent of the Data Subject must be obtained for a specific activity. Bundled consent is not considered valid consent.
Japan

Kensaku Takase
Tokyo
Tel: +813 6271 9752
kensaku.takase@bakermckenzie.com

Daisuke Tatsuno
Tokyo
Tel: +813 6271 9479
daisuke.tatsuno@bakermckenzie.com
1. Recent Privacy Developments

On 3 September 2015, extensive amendments were introduced to the law in Japan which deals with the protection of personal information, “The Act on the Protection of Personal Information” (“APPI”). The effective date of the amended APPI has not yet been fixed; however, the law will take effect two years from its date of publication. Until then, the previous APPI will continue to be the law in Japan. For purposes of this chapter, the phrase “previous APPI” refers to the APPI wording prior to the 3 September 2015 amendments.

While the details on the manner of its implementation still remain unclear, the following are some of the noteworthy amendments to the law:

a. Amended definition of “Personal Information”

The amended APPI expands the definition of “personal information” to include a person’s bodily information, such as fingerprint data and face recognition data. Numeric codes associated with an individual will also be covered by the new definition, such as passport numbers and driver’s license numbers.

b. Establishment of the Personal Information Protection Committee

A new government authority will be established, which will be called the “Personal Information Protection Committee” (the “Committee”). The Committee will have the authority to exercise certain functions, such as the ability to request data controllers to submit reports, conduct onsite inspections and issue administrative orders. How large and structured this Committee will be is still uncertain.

c. Handling of anonymized information

The amended APPI creates obligations on business operators when anonymizing personal data to be transferred to third parties. For example, a business operator must create the anonymized data pursuant to the regulations of the Committee, and ensure that the original pre-anonymized data may not be recreated.

d. Sensitive data

Under the previous APPI, there were no specific definitions concerning sensitive data such as race, religion or medical history. Under the amended APPI, business operators are prohibited from obtaining such sensitive data without the data subject’s consent. It is likely that other restrictions will also be imposed on sensitive data.

e. Transfer of personal data to third parties

Under the amended APPI, a business operator which receives personal data which has been transferred to them will need to confirm how the personal data
was obtained, and retain for a certain period, a record of when the personal data was received.

f. **Criminal sanction for the misuse of personal data**
Under the amended APPI, individuals who are involved in the handling of personal data which has been subject to misuse or which has been stolen for unjust profit will be subject to a criminal penalty.

g. **Opt-out for transfers of personal data**
Under the previous APPI, a business operator may transfer personal data to third parties without the data subject’s consent if the data subject opts-out from doing so. Under the amended APPI, a prior notification to the Committee is necessary in order to use this opt-out arrangement.

h. **Cross-border transfer of personal data**
The amended APPI provides that personal data may be transferred to a foreign country only when the country has a legal system that is deemed equivalent to the Japanese personal data protection system, or to a third party which undertakes adequate precautionary measures for the protection of personal data, as specified by the Committee.

2. **Emerging Privacy Issues and Trends**
There have been recent major data breaches in Japan, which have raised the Japanese public’s and government’s awareness of the importance of privacy issues, and the need to enhance Japan’s data protections laws.

On 9 July 2014, a Japanese education company, Benesse Holdings Inc. and its group company Benesse Corp. (“Benesse”) announced that approx. 7.9 million pieces of its customer information were leaked from its database, and that direct-mail advertisements had been sent to its customers from an unrelated IT company, which allegedly obtained the information through a broker. An engineer who was working for an outsourcing company used by Benesse was later arrested on 17 July 2014 in connection with the leak.

On 10 September 2014, Benesse announced that they will issue a 500 yen (just under USD 5) cash voucher to an estimated 28.95 million customers who were affected by the data leak. A compensation of 500-yen per customer is in line with the amount of compensation paid by Japanese companies in the past for data leak cases that were resolved outside of court. For example, in data leak cases from major convenience store franchisers, Lawson issued a 500 yen cash voucher to 5.6 million customers, and Family Mart issued a 1,000 yen cash voucher to 1.8 million customers, both in 2003. However, financial and insurance companies tend to pay more. Further, in data leak cases that were brought to court, the damage awarded by the court is even higher: 30,000 yen (plus 5,000 yen as attorney fee) per customer against TBC (major aesthetic salon operator) for the data leak in 2002, and 5,000 yen (plus 1,000
yen as attorney fee) per customer against Softbank BB for the data leak in 2006.

On 17 September 2014, Benesse submitted a final report to the Ministry of Economy, Trade and Industry (METI), following METI’s request on 10 July 2014 to submit a report under the APPI. In the report, Benesse declared that it will no longer outsource maintenance and operations of its data system to an outside company. By April 2015, Benesse will set up a new joint venture for this purpose, with a Tokyo-based information security service firm, Lac Co, one of whose directors has been a member of Benesse’s “incident investigation board” that was formed after the data leak. Further, Benesse will also establish an external body comprising of information security experts who will monitor the data management. METI plans to review the report and decide whether to issue an improvement order or take other measures against Benesse. More generally, METI plans to amend the APPI guidelines to address issues posed by the Benesse incident.

3. Law Applicable

As mentioned in Section 1, extensive amendments were introduced on 3 September 2015 to the law in Japan which deals with the protection of personal information, “The Act on the Protection of Personal Information” (“APPI”). While the effective date of the amended APPI has not yet been determined, the law will take effect two years from its date of publication.

In addition to the APPI, various guidelines have been issued by different Japanese government agencies and industry groups, which serve to ensure compliance by companies with the APPI, and to provide interpretation of the APPI as it relates to specific industries and to particular issues, such as security measures.

While the guidelines do not have any direct financial penalties for breach; non-compliance for applicable companies may have other consequences such as warnings from the agencies, or loss of regulatory licenses.

The broadest guidelines, in terms of companies covered by such guidelines, would be the Ministry of Economy, Trade and Industry’s (“METI”) guidelines on the interpretation of APPI for companies.

Other well-known guidelines include the guidelines which apply to companies in the financial, medical and telecommunications industries.

In many instances, companies may find that more than one set of guidelines are applicable to them. There are proposals to consolidate many of the guidelines to remove the overlap. However, for the time being, companies do need to be aware of which guidelines may be applicable to them.
There are also laws which separately relate to protection of personal information held by Japanese government agencies which will not be discussed in this handbook.

4. Key Privacy Concepts

a. Personal Data

The APPI applies to “Personal Information”, which is information about a living individual who can be identified by name, date of birth or other description contained in such information, including information which can easily be combined with other information so as to enable the identification of that individual.

As mentioned in Section 1, the amended APPI expands the definition of “personal information” to include a person’s bodily information, such as fingerprint data and face recognition data. Numeric codes associated with an individual will also be covered by the new definition, such as passport numbers and driver’s license numbers.

The APPI applies only to information concerning individuals, and does not cover information concerning corporations or other types of corporate entities.

The METI guidelines define “Personal Information” as information about a living individual including the name, sex and date of birth, and other personal attributes including information about one’s body, assets, occupation, and title. The guidelines further explain how Personal Information may come in various forms such as printed publications, or in visual or aural form.

Apart from “Personal Information”, “Personal Data” is separately defined to cover information stored in a business operator’s database (see the comments in Section 4(c) below with regard to a “business operator”). Such databases are defined include the following:

(i) an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer; or

(ii) an assembly of information in accordance with certain rules, and that has a table of contents, index or other means to facilitate the retrieval.

In other words, once Personal Information is stored in a database, it will be treated as “Personal Data” under the APPI. Certain provisions of the APPI deal with the broader concept of “Personal Information”, while other provisions deal with the more specific concept of “Personal Data”.

The METI guidelines give various examples of what constitutes a “database”, such as:

(i) Email address book (where combined information of names and email addresses are inputted);
(ii) Electronic files in which user IDs and log-in information on transactions by users are stored;

(iii) Business card information stored in electronic spreadsheets for business use and which can be retrieved by individuals such as workers;

(iv) Alphabetically (Japanese) arranged registration cards of temporary staff; and

(v) Commercially available directories arranged by name, address, and company.

The APPI does not distinguish between public information and privately held information.

b. Data Processing

The APPI has a very broad and open concept on data processing. “A business operator handling personal information” is interpreted to mean a business operator using a personal information database for its business.

c. Processing by Data Controllers

There is no concept of a “data processor” under Japanese law. As such, handling of personal data under the APPI should pertain to how a “business operator” treats and manages the Personal Information or Personal Data in its possession.

(i) Definition of “business operator”

The APPI uses the term “business operator” which is not defined, but essentially refers to the entity responsible for the proper handling of all “Personal Information”. This is similar to the concept of a “data controller” under EU law. It is worth noting again that there is no “data processor” concept under the APPI. In addition, the APPI does not apply to a business operator that uses a database of personal information containing personal data of less than 5,000 living individuals.

(ii) Use of Personal Information by the business operator

Once the business operator has acquired Personal Information, the business operator must promptly notify the data subject or publicly announce the “Purpose of Use” of such Personal Information. “Purpose of Use” refers to the business operators’ intended methods of use of the Personal Information. Any such use of the Personal Information by the business operator must be made within the scope of the “Purpose of Use”.

According to the METI guidelines, the public announcement must be done in a reasonable and appropriate manner depending on the nature of the business and the status of the Personal Information. Furthermore, the public announcement can be made via notices in stores, brochures, and on websites which should be easily accessible with a few clicks.
The Data Controller must not use the Personal Information beyond the scope necessary to achieve the “Purpose of Use” unless:

(i) it can obtain prior consent of the data subject; or

(ii) such use is expressly permitted under the APPI or other applicable laws.

The APPI encourages business operators to maintain accurate and up-to-date Personal Data within the scope necessary to achieve the “Purpose of Use”.

Any subsequent changes to a “Purpose of Use” must be reasonable.

d. Jurisdiction/Territoriality

The APPI does not have express provisions dealing with jurisdiction and territoriality.

e. Sensitive Personal Data

Under the previous APPI, there were no specific definitions concerning sensitive data such as race, religion or medical history. Under the amended APPI, business operators are prohibited from obtaining such sensitive data without the data subject’s consent. It is likely that other restrictions will also be imposed on sensitive data.

“The METI and FSA guidelines both define “sensitive personal data” as information relating to political opinion, religion, union membership, race, place of domicile, medical information, sexual orientation, and criminal history.

For companies which fall under the ambit of METI, the METI guidelines state that such companies should neither gather nor provide to third parties, such “sensitive personal data”. For companies which fall under the ambit of the FSA, the FSA guidelines state that such companies must treat “sensitive personal data” with caution, but does not go into further detail.

The guidelines applicable to the medical and health industry do not specifically categorize “sensitive personal data”.

f. Employee Personal Data

The APPI does not treat employee Personal Information or Personal Data any differently than any other form of Personal Information or Personal Data.

5. Consent

a. General

The general rule under the APPI is that a data subject’s prior consent is required for the transfer of their Personal Data (not for the collection of the Personal Information). However, there are exceptions to the general rule:
Subcontractor

Where a business operator entrusts the handling of Personal Data under its control, in whole or in part to another party, such a party is considered a “subcontractor” for the purpose of the APPI. For a transfer of Personal Data to a subcontractor as such, data subjects’ consent is not required. However, the business operator must exercise necessary and appropriate supervision over the subcontractor to ensure proper security management of the Personal Data.

Joint User

If the Personal Data will be jointly used by a “joint user” for the purpose of the APPI, the data subject’s consent is not required. However, the business operator must notify the data subject of the following information in advance:

(i) the fact that Personal Data is used jointly with other individuals or entities;
(ii) the items of Personal Data to be used jointly;
(iii) the scope of the joint users (i.e., the names of joint users or other information by which the Data Subject may understand who will jointly use the Personal Data);
(iv) the purpose for which the Personal Data is used by them; and
(v) the name of the individual or entity responsible for the management of the Personal Data.

Opt-Out

Under the previous APPI, a business operator may transfer personal data to third parties without the data subject’s consent if the data subject opts-out from doing so. Under the amended APPI, a prior notification to the Committee is necessary in order to use this opt-out arrangement.

Disclosure due to corporate merger

Where the information is disclosed to a surviving or newly established company following a merger or sale of a business, the surviving or newly established company receiving Personal Data is not considered a “third party”.

Others

Transfer of Personal Data to a third party is also allowed in the following circumstances:

(i) When the disclosure is made in accordance with the law;
(ii) When the disclosure is necessary to protect life, body or property (e.g., sudden illness);
(iii) When the disclosure is necessary to protect public health (e.g., epidemiology investigation); or

(iv) When the disclosure is necessary for governmental purposes (e.g., tax investigations).

b. Sensitive Data
Under the previous APPI, there were no specific definitions concerning sensitive data such as race, religion or medical history. Under the amended APPI, business operators are prohibited from obtaining such sensitive data without the data subject’s consent. It is likely that other restrictions will also be imposed on sensitive data.

c. Minors
The METI guidelines state that where a child has no ability to understand the results which may arise from his or her consent to the handling of his or her Personal Information, then it is necessary for the business operator to obtain consent from the “attorney-in-fact”, which essentially means their parent or guardian.

d. Employee Consent
As there is no special treatment in the APPI for employees, the issue of employee consent is not addressed.

e. Online/Electronic Consent:
Catch-all and preliminary consent is not allowed under the APPI. Although the APPI has no restrictions on the manner of how consent is obtained, the METI and FSA guidelines both require written consent as a general rule. Electronic consent is also recognized by both the METI and FSA guidelines as being an acceptable form of written consent.

6. Notice Requirements
Business operators are also obligated under the APPI to provide to data subjects:

(i) the business operator’s name;

(ii) the “Purpose of Use”;

(iii) the procedures used by the business operator to access, modify and terminate the use of the Personal Data it possesses; and

(iv) contact information for the purposes of handling complaints.

7. Processing Rules
See our comments under Section 4(c)(ii) with regard to Purpose of Use. Generally, a business operator must ensure that their use of Personal
Information does not extend beyond the Purpose of Use (which the data subject has agreed to in advance).

8. Rights of Individuals

The Personal Data processed by the business operators must be disclosed to the data subjects upon their request in writing or by other means acceptable to the data subjects. If retained Personal Data is found to be incorrect, such Personal Data must be corrected while remaining in compliance with the Purpose of Use.

If a Purpose of Use is found to have been violated, the Data Controller may have to discontinue using its retained Personal Data to the extent necessary to redress the violation.

If a data subject requests disclosure of his/her information or requests modifications to his/her information, the business operator must, in principle, comply with such requests unless:

(i) the disclosure is likely to harm the life, body, property or other rights or interests of the data subject or a third party;

(ii) the disclosure is likely to seriously impede the proper execution of the business of business operator;

(iii) or the disclosure violates other laws and regulations.

9. Registration/Notification Requirements

There are no requirements to notify the breach of the APPI to a government organization. However, there are special organizations set-up to specifically handle complaints relating to Personal Information on an industry level. These organizations are referred to as “Authorized personal information protection organizations” but appear to be rarely utilized at this point in time.

10. Data Protection Officers

Some guidelines, such as the METI guidelines, recommend the implementation of a data protection officer. However, such guidelines do not provide details on the role of the data protection officer other than to manage Personal Information within an organization. The Ministry of Health, Labour and Welfare’s guidelines state that organizations under their ambit should have an administrator or preferably a group of administrators who have sufficient knowledge of Personal Information issues to ensure proper management of the Personal Information they deal with.

11. International Data Transfers

The amended APPI provides that Personal Data may be transferred to a foreign country only when the country has a legal system that is deemed equivalent to the Japanese personal data protection system, or to a third party...
which undertakes adequate precautionary measures for the protection of personal data, as specified by the Committee.

12. Security Requirements

The APPI states that business operators must take necessary and appropriate measures to prevent leakage, loss or damage of Personal Data and ensure proper security management of Personal Data. This requirement is further built into industry-specific guidelines.

In particular, under the METI Guidelines, business operators are recommended to establish and manage a system to report any data security breach to:

(i) the business operator's top management;
(ii) the data subject(s) who may be affected by the breach; and
(iii) to administrative authorities.

In certain industrial sectors such as banking or financial business, the reporting of such breaches is mandatory and business operators are also required to make public announcements about the factual background as well as measures they intend to implement to prevent similar data security breach in the future.

13. Special Rules for Outsourcing of Data Processing to Third Parties

See comments under Section 5.

14. Enforcement and Sanctions

The APPI imposes sentences of imprisonment (with labor) of not more than six months, or a fine of not more than 300,000 yen for certain breaches. However, such sentences or fines may only be imposed in cases where there have been a breach of a Minister’s order made under the APPI. So far, no such orders have been made. As such, no sentences or fines have yet been made either.

15. Data Security Breach

To date, data security breaches have all been handled by companies taking the initiative and paying data subjects small amounts of compensation where breaches have occurred. There have been no instances of government agencies taking action against companies for data security breaches.

16. Accountability

Japan does not have a concept of a data processor. Accountability is with the business operator, which is similar to a data controller under EU law.
17. Whistle-blower hotline
There are no laws or regulations that govern whistle-blower hotlines in Japan.

18. E-discovery
There are no laws or regulations that govern the implementation of an e-discovery system in Japan.

19. Anti-Spam Filtering
There are no laws or regulations that govern the implementation of an anti-spam filtering system in Japan.

20. Cookies
There are no specific provisions in either the APPI or the various guidelines on usage of electronic cookies.

21. Direct Marketing
Other than general provisions dealing with transferring Personal Information to third parties, there are no specific provisions dealing with direct marketing. Please note however that sending of advertisement e-mails is regulated by a separate law named the Act on Regulation of Transmission of Specified Electronic Mail. Under this Act, advertisement e-mails may not be sent unless prior consent of the recipient is obtained.
Kazakhstan

Gulnur Bekmukhanbetova
Almaty
Tel: +7 727 330 0500
Tel: +7 727 250 99 45
gulnur.bekmukhanbetova@bakermckenzie.com

Azamat Kuatbekov
Almaty
Tel: +7 727 330 0500
Tel: +7 727 250 99 45
azamat.kuatbekov@bakermckenzie.com
1. Recent Privacy Developments

Kazakhstan has adopted a new, unified Personal Data Law ("Law") for the first time, which specifically deals with Personal Data protection issues, purports to strengthen state control over the processing of Personal Data and regulates the cross-border transfer of Personal Data. The Personal Data Law was signed into law on 21 May 2013 and came into force on 26 November 2013.

Before the adoption of the Law, Kazakhstan had only a few legal provisions relating to privacy protection, which were contained in various legislation such as the Constitution, Civil Code, Criminal Code, and the Labour Code.

The main features of the Law are as follows:

- the Law applies to all individuals, organizations (whether private-sector or state-owned) and state authorities engaged in data collection, processing or disclosure of such data within Kazakhstan;

- "Personal Data" includes any information (in paper, electronic or other form) relating to an identified or identifiable natural person ("Data Subject");

- the Law imposes a general requirement to obtain consent of the Data Subject for the collection, use or disclosure of Personal Data. There are certain exceptions to this general consent requirement, e.g., disclosure of Personal Data when required by law, use of Personal Data by state authorities for statistical purposes, etc.;

- organizations should clearly define the purpose for which they intend to collect, process and disclose Personal Data; fresh consent of the Data Subject is required for the disclosure of Personal Data if there has been a change in the purpose for which the data was originally collected;

- organizations may collect Personal Data if such data is required for the purpose of their business activities; organizations must determine the list of such Personal Data which they are allowed to collect (in accordance with government-approved rules) and distinguish the Personal Data collected from other non-private information (e.g., by way of keeping the Personal Data in separate media);

- organizations must appoint at least one person responsible for compliance with the Law;

- organizations must bring their policies and practices into compliance with the Law no later than 26 February 2014.

The Personal Data Law regulates the cross-border transfer of Personal Data. The principal rule is that Personal Data may be transferred to countries outside Kazakhstan only if they guarantee protection of Personal Data. Thus, Personal Data may in principle be transferred to countries outside Kazakhstan.
if such countries have appropriate legislation guaranteeing Personal Data protection.

There is a limited number of exceptions to this rule: specifically Personal Data may be transferred to a country that does not guarantee protection of Personal Data if, among other things:

- the Data Subject has specifically consented to the transfer of Personal Data to the relevant jurisdiction;
- the transfer of data is required as a matter of law, as a result of an overwhelming public interest, or to protect the legal rights, life and health of citizens;
- the transfer of data is necessary in specific circumstances in order to protect the legal rights of the person concerned if it is not possible to obtain the consent of the relevant Data Subject.

No exception is available for the transfer of Personal Data outside Kazakhstan within a single corporate group. Accordingly, an organization will need to rely on the above exceptions in order to transfer Personal Data of its employees, contractors and customers to a jurisdiction which is not deemed to guarantee Personal Data protection, even if such transfer occurs within a corporate group.

It is an administrative and criminal offense to collect, process and disclose Personal Data without the consent of the Data Subject or otherwise in breach of the Personal Data Law. The penalties for such an offence include financial penalties (generally, penalties of up to US$3,200 for organizations and US$32,140 for officers of organizations) or for officers of organizations - correction works, restriction of freedom or imprisonment with or without temporary deprivation of the right to hold certain positions in organizations or carry out certain activities. In addition, an individual who suffers harm as a result of an organization breaching the Law may have the right to take civil action against such organization and seek damages.

2. Emerging Privacy Issues and Trends

Mandatory Breach Notification. There is no legal requirement in Kazakhstan for organizations to notify Data Subjects when a privacy breach occurs. However, the Law allows a Data Subject to request information from an organization in order to determine how the organization has used his or her Personal Data and, where relevant, to seek to cure breaches of the Law (including by way of correcting any inaccurate information, blocking or destroying information that was collected in breach of the Law, etc.).

Data Protection Enforcement. Since the Personal Data Law was adopted recently, there is no established practice on the implementation of the Law. Specifically, it is unclear how certain provisions of the Law which are not
entirely clear will be implemented in practice, including whether it is permissible to obtain the Data Subject's consent in electronic form (in lieu of written form specifically required by the Law), whether consent of each individual business counterparty is required to collect Personal Data (such as name, identity details, and address) for the purpose of entering into a contract.

3. Law Applicable

The principal applicable laws and regulations include the following:

- Law On Personal Data and Its Protection dated 21 May 2013;
- Rules on Carrying Out Personal Data Protection Measures by the Owners and (or) Operators, as well as Third Parties approved by Government Resolution dated September 3, 2013, No. 909;
- Rules On Determining the List of Personal Data Required and Sufficient for the Owners and (or) Operators to Carry Out Their Functions approved by the Government Resolution dated 12 November 2013, No. 1214;
- Code On Administrative Offences dated 5 July 2014, as amended; and

4. Key Privacy Concepts

a. Personal Data

“Personal Data” includes any information (in paper, electronic or other form) relating to an identified or identifiable natural person (“Data Subject”);

The Labor Code defines “Personal Data” as information about the employee obtained in connection with the employment relationship. The employee’s name, address, education, pension fund related details, individual identification number, health information, and experience are considered to be the Personal Data pursuant to the Labor Code.

The Law “On Informatization” also uses the term “Personal Data,” but defines it as information on facts, events, circumstances of a person’s life and/or information allowing identification of such person.

b. Data Processing

The Labor Code and the Law “On Informatization” provide for a general rule according to which the Personal Data of an individual (whether in electronic or any other form) is deemed confidential. Recipients of the Personal Data shall use such Personal Data only for the purposes for which it was obtained. The Law “On Informatization” specifies that recipients of the electronic resources with Personal Data must keep its confidentiality starting from the moment when such data was presented.
According to the Labor Code, the employer may process Personal Data only to ensure compliance with laws and other regulations, to assist employees with job placement, training and promotion, and to ensure personal safety of the employees. The Labor Code defines the term “processing of employee’s Personal Data” as the receipt, storage and transfer of employee’s Personal Data.

Within the organization, Personal Data can be transferred in accordance with the internal rules and procedures of the employer. The employee must be familiarized with such rules and procedures. Generally, the employer may disclose Personal Data to third parties only upon the employee’s written consent. An exemption from this general rule exists when the Personal Data is disclosed to entities who, in connection with their functions, are specifically authorized to access such Personal Data. In this case, no employee’s consent is necessary, but the entities to whom the Personal Data is disclosed must keep the Personal Data confidential.

Other requirements which have to be complied with when processing the Personal Data include the following:

- an employer shall have no right to demand information regarding an employee’s political, religious and other opinions and private life; and
- an employer shall have no right to demand information regarding an employee’s membership or activity in social associations, including trade unions.

The Law “On Informatization” specifies certain aspects related to the processing of the Personal Data in electronic form. In particular, under the Law “On Informatization,” processing of the Personal Data in electronic form is generally subject to the rules and procedures established by the owner/holder of the relevant electronic resource. The owner/holder of the electronic resource that contains Personal Data is obliged to take certain “preventive” measures with respect to such electronic resources. These measures include:

- anti-disclosure measures (note: a subsequent disclosure of electronic resources that contain Personal Data is possible only upon the permission of a person to whom such Personal Data relates, or only on the grounds established by the laws of Kazakhstan);
- appropriate monitoring of the facts of unauthorized access; and
- mitigation of the consequences of various violations of the procedures regulating the access to electronic resources containing Personal Data.

In addition, the Law “On Informatization” prohibits:

- requesting, for the purpose of creation of an electronic information resource or otherwise, of information regarding the person’s private life (which information constitutes personal, family secrets, secrets of phone
conversations, mail, telegraph and other communications), origin, health, beliefs, political and religious views;

- obtaining the information referred to above without consent of the person whom the information relates to; and

- the use of electronic resources containing Personal Data to cause property and/or non-property damages or limiting rights guaranteed by laws.

c. **Processing by Data Controllers**

Please see above.

d. **Jurisdiction/Territoriality**

These rules apply only within the territory of the Republic of Kazakhstan.

e. **Sensitive Personal Data**

There is no distinction between sensitive and non-sensitive Personal Data under the Labor Code and under the Law “On Informatization.”

f. **Employee Personal Data**

Please see Sections 4(a) and 4(b).

5. **Consent**

a. **General**

Consent of the Data Subject is generally required prior to the collection, processing or disclosure of Personal Data, and is a justification or legal grounds for the use of Personal Data.

Consent must be voluntary, informed, explicit and unambiguous, and must be in writing. Consent of the Data Subject only covers identified purposes. Fresh consent is required for purposes not previously identified and consented to.

The Data Subject may be allowed to withdraw his or her consent.

b. **Sensitive Data**

Sensitive Data may only be collected and processed with the express consent of the Data Subject, except in certain prescribed circumstances.

c. **Minors**

Consent cannot be obtained from minors, but can usually be given by a legal guardian or parent.

Consent of the minor is not required to release information about him/her to parents, guardians or legal representatives.
d. **Employee Consent**

Employee consent is generally required to collect and process an employee's Personal Data, except in certain prescribed circumstances.

e. **Online/Electronic Consent**

Since the Personal Data Law was adopted recently, it is not yet clear whether it is permissible to obtain the Data Subject's consent in electronic form (in lieu of written form specifically required by the Law).

6. **Information/Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about the organization's identity, the types of Personal Data being collected, the purposes for collecting Personal Data, its privacy practices (which must be given in a clear and transparent manner), and the duration of the proposed processing.

7. **Processing Rules**

An organization that processes Personal Data must limit the use of the Personal Data to those activities that are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. **Rights of Individuals**

Data Subjects have the general right to be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed, access the Data Subject's Personal Data subject to some restrictions and/or qualifications, request the correction of the Data Subject's Personal Data, and request the deletion and/or destruction of the Data Subject's Personal Data.

9. **Registration/Notification Requirements**

There are no requirements for organizations that collect and process Personal Data to register, file or notify the local data authority.

10. **Data Protection Officers**

Organizations are required to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. **International Data Transfers**

The Personal Data Law regulates the cross-border transfer of Personal Data. The principal rule is that Personal Data may be transferred to countries outside Kazakhstan only if they guarantee protection of Personal Data. Thus, Personal Data may in principle be transferred to countries outside Kazakhstan...
if such countries have appropriate legislation guaranteeing Personal Data protection.

There is a limited number of exceptions to this rule: specifically Personal Data may be transferred to a country that does not guarantee protection of Personal Data if, among other things:

- the Data Subject has specifically consented to the transfer of Personal Data to the relevant jurisdiction;
- the transfer of data is required as a matter of law, as a result of an overwhelming public interest, or to protect the legal rights, life and health of citizens;
- the transfer of data is necessary in specific circumstances in order to protect the legal rights of the person concerned if it is not possible to obtain the consent of the relevant Data Subject.

No exception is available for the transfer of Personal Data outside Kazakhstan within a single corporate group. Accordingly, an organization will need to rely on the above exceptions in order to transfer Personal Data of its employees, contractors and customers to a jurisdiction which is not deemed to guarantee Personal Data protection, even if such transfer occurs within a corporate group.

It is an administrative and criminal offense to collect, process and disclose Personal Data without the consent of the Data Subject or otherwise in breach of the Personal Data Law. The penalties for such an offence include financial penalties (generally, penalties of up to US$3,200 for organizations and US$32,140 for officers of organizations) or for officers of organizations - correction works, restriction of freedom or imprisonment with or without temporary deprivation of the right to hold certain positions in organizations or carry out certain activities. In addition, an individual who suffers harm as a result of an organization breaching the Law may have the right to take civil action against such organization and seek damages.

12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in their possession and control are protected from unauthorized access and use; and implement appropriate physical, technical and organizational security safeguards to protect Personal Data.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data.
14. Enforcement and Sanctions
Since the Personal Data Law was adopted recently, there is no established practice on the implementation of the Law. Specifically, it is unclear how certain provisions of the Law which are not entirely clear will be implemented in practice, including whether it is permissible to obtain the Data Subject’s consent in electronic form (in lieu of written form specifically required by the Law), whether consent of each individual business counterparty is required to collect Personal Data (such as name, identity details, and address) for the purpose of entering into a contract.

15. Data Security Breach
There is no legal requirement in Kazakhstan for organizations to notify Data Subjects when a privacy breach occurs. However, the Law allows a Data Subject to request information from an organization in order to determine how the organization has used his or her Personal Data and, where relevant, to seek to cure breaches of the Law (including by way of correcting any inaccurate information, blocking or destroying information that was collected in breach of the Law, etc.).

16. Accountability
Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
Whistle-blower hotlines may be established in Kazakhstan provided that they are in compliance with local laws.

18. E-Discovery
When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of Personal Data is involved, and advise employees of the implementation of the system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.

20. Cookies
The use of cookies must comply with data privacy laws.

21. Direct Marketing
There are no laws/rules in Kazakhstan that govern direct marketing.
Luxembourg

Audrey Rustichelli
Luxembourg
Tel: +352 261844 249
audrey.rustichelli@bakermckenzie.com
1. Recent Privacy Developments

*Decision of the Luxembourg District Court n° 905/2014 of 20 March 2014 regarding the right of access of an employer to employees’ private emails*

On 20 March 2014, the Luxembourg District Court handed down a judgment expanding the right of an employer to open employees’ private emails.

An employee had been fired and was no longer required to report to work during this notice period. As a result, she was denied access to her work premises, and therefore to her emails. The employee was then informed that the emails received on her professional mailbox had been read by her former employer. The employee decided to bring proceedings against her former employer for violation of private correspondence.

The District Court considered that the employer may have a right to access the private emails of employees when these may cause confusion as regards the nature of the email. In the present case, the subject of the email was “Private. New year drink”. The judges considered that the association of these two expressions could lead to the conclusion that it was an official invitation intended for several persons.

In a second email, the object was “PRIVATE CONFIDENTIAL”. The court, however, noticed that the email had been sent from a bank to which the employer had professional relations. Therefore, the judges considered that there was only very little doubt that the employer, by opening this email sent from a professional who was then in a business relationship with the employer, had the intention to violate the legislation protecting private correspondence.

In its assessment, the Court therefore took a rather open interpretation of the scope of professional emails.

*Decision of the Luxembourg Supreme Court of 3 April 2014 relating to the theft of computer data*

On 3 April 2014, the Luxembourg Supreme Court recognized for the first time the theft of computer data. In the past, intangible property had never been considered as falling within the general legal qualification of theft under Article 461 of the Criminal Code.

The employee of a bank had downloaded and photocopied certain documents from the servers owned by his employer, a bank, for the purpose of his defense in the course of an employment-related dispute. The Supreme Court quashed the judgment of the Court of Appeal that considered that the theft was not qualified because there was no appropriation of tangible personal property from the former employee.

This decision therefore gives a larger scope to the offence of theft, as theft could now be recognized either for intangible and tangible property.
Additionally, the Luxembourg Supreme Court enshrines the principle of “exonerating circumstances”, that is to say, the act of an employee of stealing and photocopying documents or the violation of the bank secrecy laws can be considered as exonerating circumstances, provided that they are strictly necessary to exercise the right to defend himself.

*Activity report from the National Commission for the Protection of Personal Data presented on 27 May 2014 reveals a record number of complaints filed by European citizens*

On 27 May 2014, the National Commission for the Protection of Personal Data presented its activity report for 2013. The report reveals a record number of complaints or requests of verification filed from European citizens and requests of information which increased to 33% and 22% respectively compared to 2012.

These increased numbers attest to the particular sensitivity and attention of citizens regarding privacy and protection of their personal data. The complaints notably concern requests for deletion or correction of the personal data and questions on the lawfulness and validity of certain administrative or commercial practices.

Additionally, certain requests introduced by citizens established on another European Country triggered investigations handled by the Luxembourg data protection authority towards international companies established in the Grand-Duchy of the Luxembourg.

*Joint publication in September 2014 of the surveillance at the workplace by the National Commission for the Protection of Data and the Chamber of Employees regarding*

In September 2014, the National Commission for the Protection of Data (“CNPD”) and the Chamber of Employees published new guidelines regarding the surveillance of employees at their workplace. This publication echoes the decision of the Luxembourg District Court of 20 March 2014 regarding the access of an employer to private emails of his employees. In this respect, the judges notably ruled that an employer may have a right to access the private emails of employees when these emails may be confusing as regards their private or professional qualification.

The Luxembourg legislator has created a quite restrictive framework regarding the implementation of processing of personal data for surveillance purposes. The publication aims at analyzing the different forms of surveillance that could occur at the workplace, such as video surveillance, the control of the use of IT tools or the recording of telephone conversations and provides requirements applicable to these types of surveillance as well as best practices.
The document also contains guidelines for employers and employees on the use of IT tools, and in particular of the professional mailbox. Namely, the CNPD provides that employers should ask employees to:

- clearly distinguish the private from the professional emails in the subject of the messages;
- install a double mailbox separating the private and professional emails;
- archive the personal emails in a file called “private”.

Publication on 10 September 2014 from the National Commission for the Protection of Data regarding the right to oblivion

On 10 September 2014, the CNPD published practical guidelines regarding the right to oblivion.

The right of oblivion is the possibility given to a data subject to request that the processing of his/her personal data be discontinued and that the related data be removed. Contained in the law of 2 August 2002, as amended, regarding the Protection of Persons with regard to the Processing of Personal Data, this right can however only be exercised by showing compelling and legitimate reasons relating to the special situation of the data subject. This means that the data subject has to show that the processing of his/her personal data is contrary to the legal principles of necessity, relevance and legitimacy of the processing.

In September 2014, the CNPD provided practical useful guidelines regarding the request for deletion of personal data from a specific website on the Internet and also from search engines. Forms are available online for such requests. Website administrators and search engine operators have one month to answer by making a balance between the legitimate interest of the web surfers to accessing certain links/information and the fundamental rights of the person concerned and, if negatively answered, to justify such refusal. The data subject may, in such case, contact the CNPD asking the authority to intervene.

Such practical steps should help data subjects in the exercise of their right to oblivion which, until now, has been very rarely used by individuals.

2. Emerging Privacy Issues and Trends

Internet of Things: Following the development of an increasing number of devices connected to the Internet and the security issues arising from this new trend, the CNPD is paying close attention to the Internet of Things. In a publication in December 2014, the authority highlighted the risks to privacy, as well as the impact on the protection of personal data of data subjects and mentioned tools that can be used which will provide protection when using such devices.
Privacy by design: A current point of focus and discussion of actors in privacy matters is the question of privacy by design. This concept refers to a way of protecting privacy by embedding it into the design specifications of technologies, business practices, etc. and decreasing the risk of security as regards to the processing of personal data of users. Following this approach, data protection safeguards should be built into products and services from the earliest stage of development. This issue has notably been addressed by the European Commission in their proposal for a General Data Protection Regulation.

3. Law Applicable

The applicable law is the law of August 2, 2002, as amended, on the Protection of Persons with regard to the Processing of Personal Data (“Law of 2002”).

Further data protection provisions are contained in legislation regulating specific sectors such as the law of July 28, 2011 amending the law of May 30, 2005 concerning the protection of privacy in the electronic communication sector.

4. Key Privacy Concepts

a. Personal Data

The Law of 2002 applies to any information (“Personal Data”) of any type regardless of the type of medium, including sound and image, relating to an identified or identifiable natural person (“Data Subject”). Natural persons will be considered to be identifiable if they can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to their physical, physiological, genetic, mental, cultural, social, or economic identity.

b. Data Processing

“Processing” is widely defined and covers any operation or set of operations performed on Personal Data, whether or not by operated means, such as the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as blocking, erasure or destruction of Personal Data.

c. Processing by Data Controllers

The Law of 2002 applies to a natural or legal person, public authority, agency or any other body other than the Data Subject which, solely or jointly, determines the purposes and methods of processing Personal Data (“Data Controller”).
d. Jurisdiction/Territoriality

The Law of 2002 only applies:

- if the Data Controller is established in the territory of the Grand Duchy of Luxembourg; or

- if the Data Controller is not established in Luxembourg nor in another EU member State, but involves “equipment of processing” based in Luxembourg territory, apart from equipment that is used only for the purposes of transit through the said territory.

e. Sensitive Personal Data

As a principle, the processing of sensitive Personal Data - that is, data relating to racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, or health or sexual life is prohibited.

However, the Law of 2002 provides a list of exceptions to this prohibition. Sensitive Personal Data may be processed if:

- the Data Subject has given his/her express (i.e., written) consent subject to certain restrictions;

- the processing is necessary for the purpose of carrying out the obligations and specific rights of the Data Controller in the field of employment law in so far as it is authorized by law;

- the processing is necessary to protect the vital interests of the Data Subject or another person, where the Data Subject is physically or legally incapable of giving consent;

- processing is carried out with the consent of the Data Subject by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade union aim in the course of its legitimate activities and on condition that the processing relates to the necessary data solely of members of that body or to persons who have regular contact with it in connection with its purposes and that the data is not disclosed to third parties without the consent of the Data Subject;

- the processing relates to data that have been clearly made public by the Data Subject;

- the processing is necessary to acknowledge, exercise or defend a right at law;

- the processing is necessary in the public interest for historical, statistical or scientific reasons;

- the processing is implemented via a specific Luxembourg regulation, such as the processing of operations relating to State security, defense and public safety; or,
• the processing is implemented in the context of the processing of legal data; i.e., the processing of data for the purpose of criminal investigations and legal proceedings and data related to offenses, criminal convictions or security measures.

There are specific additional requirements in relation to the processing of genetic data and the processing of specific categories of data by health-related services.

f. Employee Personal Data
The Law of 2002 does not provide for specific rules regarding employee Personal Data.

When such data is likely to include Sensitive Personal Data (e.g., health-related information), the data may be processed in the circumstances mentioned in Section 4(e) above and, in particular, for the purpose of carrying out the Data Controller’s obligations under employment law.

5. Consent
a. General
Consent of the Data Subject is not specifically required by Luxembourg law. It is, however, considered as a justification for the collection, processing and use of Personal Data. Written consent is not required, except for Sensitive Data.

When a Data Subject gives consent, it is understood to only cover the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to. In addition, a Data Subject has the right to withdraw consent at any time in given circumstances.

b. Sensitive Data
Where consent is relied upon to justify the processing of Sensitive Personal Data, it must be explicit and must be either written or obtained by a double-click, if consent is given over the Internet.

c. Minors
Minors under the age of 18 cannot give valid consent. The consent of a parent or guardian is required on their behalf. Further, the parent or guardian has the right to be informed of the collection of information and to access and rectify the Personal Data.

d. Employee Consent
While consent of employees is not specifically required by Luxembourg Law, the Article 29 Working Party has produced an opinion on the processing of Personal Data in the employment context which states that it is not appropriate for an employer to try to rely on an employee’s consent as it is unlikely to be freely given.
The CNPD has raised doubts as to whether consent given in the context of an employment relationship can be considered valid. There is a risk that the employee may feel forced to consent.

e. Online/Electronic Consent

In the case of non-sensitive Personal Data, consent may be given electronically, and will be considered to have been properly demonstrated where it can be shown that the Data Subject had sufficient notice of the requisite information forming the basis of consent (e.g., inclusion of a notice or policy in a box directly above a consent button) and steps have been taken to prevent consent from being mistakenly given (e.g., a double click acceptance process). Where written consent is required by law (e.g., regarding Sensitive Data), further requirements need to be met.

6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be provided in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not giving consent; the rights of the Data Subject; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to contact the privacy officer or other person who is accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; and how to access and/or correct the Data Subject’s Personal Data.

7. Processing Rules

An organization that processes Personal Data must: limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and of how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

Data Controllers must notify the CNPD prior to the processing of Personal Data. The Law of 2002 provides for a list of cases where the Data Controller is exempt from the notification requirement. The exemption mainly applies to the
processing of data concerning employees wages and/or payroll, as well as clientele management, bookkeeping, and the administration of shareholders.

10. Data Protection Officers

The appointment of a data protection officer is possible but is not mandatory. Should a data protection officer be designated by the Data Controller, specific formalities defined by the Law of 2002 will apply. There is no requirement for such officer to be located in Luxembourg.

11. International Data Transfers

Transfers of Personal Data from Luxembourg to EEA Member States are generally permitted without the need for further approval. The same applies to transfers to Andorra, Australia, Faeroe Islands, Switzerland, Israel, Jersey, Guernsey, Argentina, the Isle of Man, and Canada.

Data from the EEA may only be freely sent to the United States to companies which have voluntarily adhered to the Safe Harbor arrangement.

The Data Controller may transfer the Personal Data to a state not offering a sufficient level of protection of privacy in the following cases:

- the Data Subject has given consent to the proposed transfer;
- the transfer is necessary for the performance of a contract to which the Data Subject and the Data Controller are parties or which has been concluded in the interest of the Data Subject between the Data Controller and a third party;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of a legal claim;
- the transfer is necessary in order to protect the vital interests of the Data Subject; or
- the transfer occurs from a public register.

According to the Article 29 Working Party, the above-mentioned conditions must be interpreted strictly.

Without prejudice to the exceptions listed above, the transfer of Personal Data to a “non-safe” country is legal if it has been authorised beforehand by the CNPD. Such authorisation is granted only if the following conditions are met:

- Initial processing of Personal Data complies with the Law of 2002: the initial processing of Personal Data has to comply with the requirements related to the quality and security of the Personal Data processed, the legitimacy of the processing, and the information of the data subject; and
• Contractual clauses: the CNPD’s authorization to transfer the Personal Data to a “non-safe” country may be granted if the Data Controller offers sufficient guarantees in respect of the protection of privacy, freedoms and fundamental rights of the Data Subjects, as well as the exercise of the corresponding rights and that these guarantees may result from appropriate contractual clauses.

The CNPD will always accept data transfer agreements incorporating the model contractual clauses approved by the European Commission for transfers from Data Controller to Data Controller or from Data Controller to data processor.

Alternatively, another form of securing the transfer of Personal Data within the same corporate group consists in applying binding corporate rules ("BCR") with which any organization of the group will need to comply.

The general rules concerning the legality of processing must always be fulfilled.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

According to the Law of 2002, any processing carried out on another's behalf must be governed by a written contract (data processing agreement) or legal instrument binding the data processor to the Data Controller and providing in particular that:

• the Data Processor will act only on instructions from the Data Controller, and

• the Data Processor has the obligation to implement adequate appropriate technical and organizational measures.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.
15. Data Security Breach

There is no legal obligation to notify data security breaches under the Law of 2002. The Data Controller could, however, always decide, depending on the importance of the breach, to inform the authority or the affected individual on a voluntary and purely informative basis, based on an internal management decision and not as a consequence of a legal requirement. The only existing obligations to provide notice of a breach of security is in the sector of electronic communications and networks. A specific form allowing a Data Controller to notify of data security breaches is available on the website of the National Commission for Data Protection.

An organization that is involved in a data breach situation may be subject to closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, or civil actions and/or class actions.

16. Accountability

There is currently no law/regulation/guidance materials in Luxembourg that mandates organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-blower hotline

The Law of 2002 is silent with respect to whistle-blower hotlines. On 11 May 2009, the CNPD published on its website, a “thematic file” on the issue and indicated that their position is in line with the Opinion WP 117 issued by the Article 29 Working party on 1 February 2006.

Nevertheless, a whistle-blowing system has to be notified to the CNPD beforehand.

Should the system imply the permanent monitoring of employees by technical instruments, the filing of a prior authorization is also needed.

18. E-discovery

An organization implementing an e-discovery system is not required to obtain the consent of employees even if the collection of Personal Data is involved. The organization is also not mandated to advise employees of the implementation of an e-discovery system, the monitoring of work tools, and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace. Spam-filtering solutions will need to comply with applicable data protection laws. A notification will need to be filed before
the CNPD. Additionally, the storage and access to location and traffic data must be performed in compliance with the Law of 2011.

20. Cookies

There are specific laws/rules that regulate the deployment of cookies; and hence, the use of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. An organization must obtain consent for a specific activity. Bundled consent is not considered valid consent.
Malaysia

**Woo Wei Kwang**  
Kuala Lumpur  
Tel: +603 2298 7898  
weikwang.woo@wongpartners.com

**Ken Boon Low**  
Kuala Lumpur  
Tel: +603 2298 7988  
kenboon.low@wongpartners.com

**Shameen Mohd. Haaziq Pillay**  
Kuala Lumpur  
Tel: +603 2298 7943  
shameen.mohd.haaziqpillay@wongpartners.com
1. Recent Privacy Developments

The Malaysian Personal Data Protection Act 2010 ("PDPA") came into force on November 15, 2013 together with various regulations.

These are the Personal Data Protection Regulations 2013 ("Regulations"), Personal Data Protection (Class of Data Users) Order 2013, Personal Data Protection (Fees) Regulations 2013, and the Personal Data Protection (Registration of Data User) Regulations 2013.

Prior to the coming into force of the PDPA, information of a personal nature was protected only as confidential information through sectoral secrecy obligations, contractual obligations or the common law.

The PDPA seeks to govern the previously unregulated area of personal data processing by data users in the context of commercial transactions, and to provide safeguards for data subjects such as consumers, employees and e-commerce users. “Commercial transactions” are defined broadly to encompass transactions of a commercial nature, whether contractual or not, and include matters relating to the supply or exchange of goods and services, agency, investment, financing, banking and insurance. There was a 3-month transitional period for compliance in respect of Personal Data collected prior to the PDPA coming into force. The PDPA is a Code of Practice ("Code")-based regime, but no Codes have thus far been introduced.

2. Emerging Privacy Issues and Trends

(a) Codes, with the force of law under the PDPA have yet to be issued.

(b) The Codes are expected to formally clarify the following issues among others:

(i) how data subject consent, which must be recorded and maintained properly by the data user, may be implied and generally obtained and in what situations;

(ii) clarification on the exemption from obtaining data subject consent where the processing is necessary for the performance of a contract to which the data subject is a party to;

(iii) similarly, clarification on the exclusion for personal data processed in the course of “discharging regulatory functions”;

(c) Detailed standards are expected to be issued relating to compliance with the Security, Retention and Data Integrity Principles.
At present, the Personal Data Protection Commissioner ("Commissioner") has not made any official announcements, but we would expect the following issues to be dealt with as data users and data subjects become more familiar with the concept of personal data privacy:

(i) employee monitoring;

(ii) implied data subject consent;

(iii) retaining or otherwise processing the information stored within the data subject’s national identification card; and

(iv) clarification on personal data contained in business cards. The PDPA has no business information-related exceptions.

3. Law Applicable

The PDPA, which came into force on November 15, 2013 together with various regulations.

These are: the Personal Data Protection Regulations 2013, Personal Data Protection (Class of Data Users) Order 2013, Personal Data Protection (Fees) Regulations 2013, and the Personal Data Protection (Registration of Data User) Regulations 2013.

4. Key Privacy Concepts

The PDPA sets out a broad framework for the protection of personal data. The scope and application of the PDPA will be fleshed out through Codes.

a. Personal Data

Under the PDPA, “personal data” means any information in respect of commercial transactions which:

• is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;

• is being recorded with the intention that it should wholly or partly be processed by means of such equipment; or

• is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;

and that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expressions of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.
There are seven data protection principles which form the basis of protection of Personal Data under the PDPA. The principles are as follows:

- General Principle;
- Notice and Choice Principle;
- Disclosure Principle;
- Security Principle;
- Retention Principle;
- Data Integrity Principle; and
- Access Principle.

b. Data Processing

The scope of the PDPA extends to personal data that is recorded in a form which may practically be processed by any automatic means or otherwise, including both electronic and manual processing. If the information is not recorded (e.g., in oral form or manual unconsolidated data), it will be excluded from the scope of the PDPA. "Processing" is defined under the PDPA as collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including the:

- organization, adaptation or alteration of personal data;
- retrieval, consultation or use of personal data;
- disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or
- alignment, combination, correction, erasure or destruction of personal data.

c. Processing by Data Processors

The PDPA defines a “data user” as a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor.

Note that a person who merely collects, holds, processes or uses personal data solely on behalf of another person, and not for any of his own purposes may be construed as “data processor” under the PDPA. There are different requirements applicable to ensure that the personal data processed by data processors is protected.
d. **Jurisdiction/Territoriality**

The scope of the PDPA only extends to personal data that is processed in Malaysia. The PDPA will not apply to any personal data processed outside Malaysia, unless the personal data is intended to be further processed in Malaysia.

While it is not expressly stated in the PDPA, it is likely that the legislation will only apply to living individuals. Personal Data processed only for the purpose of an individual’s personal, household affairs and for recreational purposes is exempted from the PDPA.

In addition, the Federal and State governments are excluded from the PDPA. Credit reporting or referencing agencies are separately regulated by the Credit Reporting Agencies Act 2010.

e. **Sensitive Personal Data**

Under the PDPA, “sensitive personal data” is defined broadly as any personal data consisting of information as to the physical or mental health or condition of a data subject, his/her political opinions, his/her religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him/her of any offense or any other personal data as the Minister may determine by order published in the *Gazette*.

The PDPA prohibits any person from collecting, holding, processing or using any sensitive personal data unless the data subject has given his or her explicit consent. Exceptions include where the processing of sensitive personal data is required for the administration of justice or for medical purposes.

f. **Employee Personal Data**

The scope of the PDPA is only limited to commercial transactions. Notwithstanding that an employment relationship is not typically regarded as a “commercial transaction”, the Personal Data Protection Department ("Regulator") has verbally confirmed that the provisions of the PDPA apply to employers who process employee personal data.

5. **Consent**

a. **General**

The PDPA prohibits the processing of personal data without the consent of the data subject for any purpose other than the purpose for which the personal data was to be used at the time of its collection, unless such other purpose is directly related to the purpose for which the personal data was to be used at the time of its collection.
Consent of the data subject is not necessary if the use of the personal data falls under any of the following exceptions:

- performance of a contract to which the data subject is a party;
- for the taking of steps at the request of the data subject with a view to entering into a contract;
- compliance with any legal obligation of which the data user is the subject, other than an obligation imposed by a contract;
- protection of the vital interests of the data subject;
- administration of justice; or
- exercise of any functions conferred on any person by or under any law.

The PDPA does not specify the form or nature of the consent and whether consent can be implied by conduct (but see discussion below regarding “explicit consent” for the processing of sensitive personal data).

The data subject also has the right to withdraw consent at any time in any given circumstances.

b. Sensitive Data

“Sensitive personal data” requires “explicit” data subject consent. “Sensitive personal data” includes medical history, religious beliefs, political opinions and the commission or alleged commission of any offense. “Explicit consent” implies that such consent must be in writing and that relatively more detailed information from the data user will be required before the consent can be regarded to be sufficient. This also indicates that under the PDPA, consent with regard to (non-sensitive) personal data need not always be in writing and can be implied.

Explicit consent is not required in certain circumstances – for example, the use or disclosure of data is necessary to protect the vital interests of the data subject or another person. Otherwise, the processing of the data is prohibited.

“Explicit consent” implies that such consent must be in writing, and that there must be an additional level of detail relating to the purpose of the processing. This also indicates that consent with respect to the processing of non-sensitive personal data can be implied.

c. Minors

The Regulations provide that in respect to the processing of the personal data of a person who is under the age of 18, consent is to be obtained from the parent, guardian or the persons with parental responsibility.
d. **Employee Consent**

Under the PDPA, the consent of employees (as data subjects) need to be obtained for the processing of the employees' personal data (which includes sensitive personal data).

e. **Online/Electronic Consent**

In Malaysia, electronic consent is permissible and enforceable provided that it is properly structured and evidenced.

In relation to commercial contracts, the Malaysian Electronic Commerce Act 2006 ("MECA") expressly provides that any information shall not be denied legal effect, validity or enforceability on the ground that it is wholly or partly in an electronic form. Note, however, that the MECA applies only to commercial contracts and not to personal data in particular.

While there is no provision in the PDPA that specifically addresses online/electronic consent, the Regulator has verbally confirmed that this is permissible for purposes of the PDPA.

6. **Information/Notice Requirements**

An organization that collects personal data must provide data subjects with information about the organization’s identity; the description of the personal data processed; the purposes for collecting and further processing the personal data; the source of the personal data; third parties to which the organization will disclose the personal data to; whether it is obligatory or voluntary for data subjects to supply the personal data and if obligatory the consequences of not providing consent; the rights of data subjects to request access to and correct of their personal data and how to contact the data user or a contact person within the organisation in order to make an inquiry or file a complaint; and of the data subjects’ right to limit the processing of their personal data.

7. **Processing Rules**

An organization that processes personal data must limit the use of the personal data to only those activities which are necessary to fulfill the identified purpose(s) for which the personal data was collected, and delete/anonymize personal data once the stated purposes have been fulfilled and legal obligations met.

8. **Rights of Individuals**

Data subjects have the general right to: be informed by an organization of the personal data the organization holds about the data subject and how the personal data is being processed; access their personal data subject to some restrictions and/or qualifications; request the correction of their personal data; and request the deletion and/or destruction of their personal data.
9. Registration/Notification Requirements

Organizations that collect and process personal data may be required to register with the Regulator.

Certain classes of data users are required to register with the Regulator. These include, among others, licensed banks, insurers, private health care institutions, licensed tour operators, direct sales businesses, private higher education institutions and certain utilities and transportation service providers. These data users have a 3-month period from enforcement to register. Data users who fail to do so may be liable for a fine of up to RM500,000 and/or a term of imprisonment of up to 3 years. Directors, managers and other responsible persons may be found to be jointly liable with the non-complying data user. The Commissioner is not empowered to order compensation for damage suffered, and there is no express right to pursue a civil claim for non-compliance.

10. Data Protection Officers

The PDPA is silent as to whether organizations are required to designate a privacy officer or any other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

The PDPA prohibits data users (and by extension, their data processors) from transferring any personal data of a data subject to a place outside Malaysia, unless:

- it is to a place specified by the Minister and published in the Gazette;
- the data subject has given his or her consent; or
- any other general exemptions apply.

The factors that the Minister will take into consideration include: whether or not that place has in force any law which is substantially similar to the PDPA or serves the same purposes as the PDPA and whether that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA. No places have been so specified by the Minister yet.

12. Security Requirements

Organizations are required to take steps to ensure that personal data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect personal data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the personal data involved.
Regulations now mandate that all data users must develop and implement a security policy.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose personal data to third parties are required to use contractual or other means to protect personal data, and are required to comply with applicable sector specific requirements. Organizations may, depending on the particular circumstances, be liable together with third party providers in cases of breaches by the latter.

Under the PDPA, where a data processor processes personal data on behalf of the data user, the data user shall, for the purpose of protecting the personal data from any loss or misuse, ensure that the data processor:

(a) provides sufficient guarantees in respect of the technical and organizational security measures governing the processing; and

(b) takes reasonable steps to ensure compliance with those measures.

The PDPA does not prescribe the entering of a data transfer agreement, nor does it prescribe the contents of such agreement.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, and/or criminal proceedings, which could result in imprisonment of the directors, managers and other persons responsible if the data user is found guilty.

15. Data Security Breach

At present, there is no positive obligation to notify the Regulator or data subjects in the event of a security breach. Such notification may, however, be taken into account when assessing whether the data user has complied with the Security Principle.

A breach of any of the data protection principles is an offence under the PDPA and is punishable by a fine of up to RM300,000, and/or a term of imprisonment of up to two years.

16. Accountability

Organizations are not legally required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of personal data.
17. Whistle-Blower Hotline
Whistle-blower hotlines may be established in Malaysia as long as they are in compliance with local laws.

18. E-Discovery
When implementing an e-discovery system, an organization may be required to obtain the consent of the employees if the processing of personal data is involved, and to advise employees of the implementation of the system, workplace surveillance and on the storage of information.

19. Anti-Spam Filtering
Under the Communications and Multimedia Act 1998 ("1998 Act"), it is an offense for any person to intercept, attempt to intercept or procure any other person to intercept or attempt to intercept, any communications including communication via electronic means. It is possible that a spam-filtering solution installed by an employer may be tantamount to intercepting its employees’ communications. The issue of whether or not the employees had given consent is irrelevant under the 1998 Act. Nevertheless, it is not uncommon for large organizations to implement a spam-filtering system whereby suspected spam e-mails are isolated.

A general spam filter should not fall foul of the 1998 Act, when the system merely gives the receiver of suspected spam e-mail the option to allow these spam e-mails to be forwarded to his or her inbox and to create rules that future e-mails from the same e-mail account will not be filtered.

20. Cookies
There are no specific laws/rules in Malaysia that regulate the use and deployment of cookies. In general, the use of cookies is valid as long as it complies with data privacy laws.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a data subject is required to obtain the data subject’s prior consent, which may not be inferred from a data subject’s failure to respond.
Mexico

Sergio Legorreta-Gonzalez  
Mexico City  
Tel: +52 55 5279 2954  
sergio.legorreta-gonzalez@bakermckenzie.com

Carlos Vela-Trevino  
Mexico City  
Tel: +52 55 5279 2911  
carlos.vela-trevino@bakermckenzie.com
1. Recent Privacy Developments

**Protection of children’s honor and reputation in the media**

On December 4 of 2014, Mexico enacted the General Law for Children and Teenagers (“GLCT”). The GLCT includes a new chapter that deals with the protection of children and teenager’s privacy. Section 77 of the GLCT sets forth that any use of children’s image, name or personal data in media channels (including, radio, television, Internet and printed media) may be considered as a privacy breach where personal data of the minors are depicted in ways that may affect their honor or reputation, affect their rights, or place minors in a risky situation. Media concession holders that exercise control over the media channels or network may be subject to fines in case of breach to this provision.

**Guidelines for appropriate personal data processing by debt collection companies**

Debt collection services firms had been subject to enormous criticism during the last 10 years due to their poor and unethical collection practices. The proliferation of these firms together with constant claims filed by consumers (more than 200,000 claims between 2007 and 2014) have caused the IFAI and the National Commission for the Defense or Financial Consumer Services to issue on November 17, 2014 the *Guidelines for appropriate personal data processing by debt collection companies*. Under this document, firms are prohibited to call family members of work colleagues of debtors. They must identify themselves clearly during the collection process, provide information about the existence of the privacy notice each time a collection call is made, and take proactive measures to ensure the quality of debtor’s databases.

2. Emerging Privacy Issues and Trends

**Enforcement by authorities different than the Data Protection Authority.**

On November 3, 2014, the Consumer Protection Authority (PROFECO) enforced for the first time privacy and information security provisions contained in the Federal Consumer Protection Law and imposed fines of around $300,000 on 8 online retailers. Enforcement by authorities other than the IFAI on issues related to privacy and information security has caused significant concerns among the private sector, which has urged IFAI and PROFECO to adopt a similar and consistent criteria and approach for the interpretation of privacy laws and regulations.

**Debt Collection processes** - Claims filed by the data subjects opposed to poor handling of personal data carried out by debt collection firms have resulted in fines imposed on banks that hired such firms since banks are considered as responsible for the poor handling of personal data carried out by their contractors. The number of these claims are expected to increase during 2015.
3. Applicable law

Legal Framework:
- Constitution of the United Mexican States (Articles 16 and 73);
- Federal Law on Protection of Personal Data Held by Private Parties;
- Regulations to the Federal Law on Protection of Personal Data Held by Private Parties

Publications:
- Recommendations in matters of Personal Data Security
- Practical guideline to generate a Privacy Notice;
- Practical guideline to attend the Rights ARCO;
- Recommendations to designate the Chief Privacy Office

4. Key Privacy Concepts

a. Personal Data
Any information that refers to an identified or identifiable individual is considered to be personal data (“Personal Data”) under the Data Protection Law. The definition includes information of, among others, any of the following groups:
- customers and potential customers;
- suppliers/vendors/entity partners;
- employees; and
- Other third parties/competitors.

b. Data Processing
The term “data processing” means the collection, use –access, handling, profiting, transferring and disposal–, disclosure and storage of Personal Data and therefore comprises the whole life cycle of Personal Data processed within an organization. As a general rule, data subject’s consent is required for any data processing activity. The Law applies to Personal Data held both in hard-copy and electronically and to both manual and automated handling of data.

c. Processing by Data Controllers
A Data Controller (“Data Controller”) is an individual or an entity that takes the decisions regarding the processing of Personal Data. Under the "Responsibility Principle" embraced by the Law, a Data Controller is responsible for complying with the obligations and data protection principles.
set forth by the Law, even if such data is transferred to a Data Processor, to an affiliate or to a third party, being such parties located in Mexico or abroad. A Data Processor (“Data Processor”) is an individual or an entity that solely or jointly with others, processes Personal Data on behalf of the Data Controller. The Data Processor, in order to be legally considered as such, should be a third party (i.e., it should not be an entity related to the Data Controller or from the same corporate group) and must operate under an agreement.

Since July 6, 2011, all Data Controllers have two notable obligations:

1. All Data Controllers must deliver privacy notices to data subjects before the data is collected and:

2. All Data Controllers must create within their organization a data protection function, either by appointing a Chief Privacy Officer or by creating a Data Protection Department.

Data subjects are entitled to file before the Data Controller’s Data Protection Departments, requests related to ARCO rights. Privacy Departments must receive and process such requests, analyze if the petitions must proceed and resolve such request within specific timeframes set forth by the Law.

Data Controllers are required to develop compliance programs and to allocate resources in order to strengthen the privacy function.

d. Jurisdiction/Territoriality

The Data Protection Law is applicable to any individual or entity having a legal domicile or local office or branch in Mexico, or where the managed databases are located in Mexico. However, data protection rules apply also to Data Controllers not based in Mexican territory, if such entities use, for the processing of Personal Data, means located within the Mexican territory. In such a case, the Law provides that the Data Controller, even if located abroad, shall incorporate the necessary mechanisms to comply with the Law.

e. Sensitive Personal Data

In Mexico, Sensitive Personal Data encompass any data that may affect the inner core intimacy of the data subject. Certain data is considered per se as sensitive Personal Data: data that reveals racial or ethnic origin, present or future health conditions, genetic information, religious, philosophic or moral beliefs, union affiliation or sexual preference should at all times be considered as sensitive data. However, other types of data could be considered as sensitive upon a specific context. In this regard, Personal Data that if wrongly used may place the data subject in a dangerous situation or in a position of being subject to discrimination should be considered also as sensitive data.
In general, the processing of Sensitive Personal Data is subject to more stringent rules. Fines that could be imposed if an entity fails to comply with applicable rules are twice as much, when breaches relate to Sensitive Personal Data.

f. Employee Personal Data
There is no special regime applicable to employees, as data subjects, under the Personal Data Law. Therefore, general rules apply to employees.

5. Consent
a. General
Consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances.

Consent is generally contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is usually understood to only cover the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

Consent must be in the local language to be valid.

b. Sensitive Data
Mexican law recognizes Sensitive Data as a special category of Personal Data. It is subject to additional and special consent requirements. While Sensitive Data may only be collected and processed with the express consent of the Data Subject, Sensitive Data may be processed without obtaining consent in certain prescribed circumstances.

c. Minors
While consent from minors is not specifically addressed in any law, the general rule is that minors are considered incapable of giving consent. However, parents or legal guardians of minors are allowed to provide consent on behalf of the minor.

d. Employee Consent
The general rule is that employee consent is required to collect and process an employee’s Personal Data; however, there are instances when employee consent is not required, e.g., to carry out an employment contract or administer an employment relationship, or to fulfill a legitimate interest of the employer.
e. **Online/Electronic Consent**

In Mexico, online or electronic consent is permissible and deemed effective if properly structured and evidenced.

6. **Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity, the types of Personal Data being collected; the purposes for collecting Personal Data, its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the rights of the Data Subject; where the Personal Data is to be transferred; how to contact the privacy officer or other person who is accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; and how to access and/or correct the Data Subject’s Personal Data.

7. **Processing Rules**

An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; anonymize the Personal Data whenever possible; provide the Data Subject the option to use a pseudonym or remain anonymous whenever possible; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. **Rights of Individuals**

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. **Registration/Notification Requirements**

An organization that collects and processes Personal Data is not required to register, file and notify the appropriate data authority.

10. **Data Protection Officers**

In Mexico, organizations are required to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.
11. International Data Transfers

Organizations may transfer Personal Data outside of Mexico provided that impacted Data Subjects have been informed or have provided consent, and that reasonable steps have been taken to safeguard the Personal Data to be transferred.

Organizations may transfer Personal Data outside of Mexico provided that appropriate data transfer agreements (e.g., Model Contractual Clauses) or other prescribed measures are put in place; or binding corporate rules (“BDRs”) are implemented to secure international data transfers.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors. In case of an occurrence of data breach, the outsourcing organization may be held liable together with the third party provider.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

Organizations that are involved in a data breach situation are required to comply with mandatory data breach notification requirements, notify impacted Data Subjects depending on the scope of the breach; gather information about the breach; assess the potential risk of harm to the Data Subjects, take steps to mitigate the harm to impacted Data Subjects; take steps to contain the breach and to prevent future similar breaches; and comply with data authority orders and court orders. Depending on the nature and scope of the breach, the organization is not required to notify the data authority.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions and/or class actions.
16. Accountability
In Mexico, organizations are required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. Subject to regulatory guidance, organizations may be required to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

17. Whistle-blower hotline
Whistle-blower hotlines may be established in Mexico provided that they are in compliance with local laws.

18. E-discovery
When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of Personal Data is involved; and advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.

20. Cookies
There are specific laws/rules that regulate the deployment of cookies, and hence, the use of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. Opt-out consent is permissible.
Netherlands

Remke Scheepstra
Amsterdam
Tel: +31 20 5517 831
remke.scheepstra@bakermckenzie.com

Wouter Seinen
Amsterdam
Tel: +31 20 5517 161
wouter.seinen@bakermckenzie.com
1. Recent Privacy Developments

**Legislative bill introducing a general data breach notification duty and increasing the maximum penalties**

A legislative bill, with chamber number 33 662, was submitted in 2013 and is designed to amend the Dutch Personal Data Protection Act (“Wet bescherming personengegevens”) (the “PDPA”) and some other affiliated legislation. The aim of the bill is to impose a duty on data controllers to report data security incidents to the Dutch Data Protection Authority (“DPA”), if such incident is likely to have caused a breach of personal data. Under the bill, data subjects must also be notified if the data breach at hand is likely to have adverse an impact on their privacy.

In addition, the bill increases the maximum penalties for violations of the PDPA. It provides for imposition of administrative fines of up to EUR 810,000 or 10% of the national annual turnover for failure to comply with the rules of the PDPA. The increased maximum penalty will also apply to the new data breach notification obligations.

The bill will take effect per 1 January 2016.

**New draft bill on data breach notification duties for providers of critical infrastructure**

On 22 January 2015, a draft of another new bill was published. This bill aims to introduce a specific data breach notification duty for businesses and governmental bodies that provide critical infrastructure. Under the proposed bill, such providers will be required to report data breaches and data security incidents to the National Cyber Security Centre (“NCSC”).

This notification duty is not limited to breach of personal data but also applies to loss of other data and security incidents such as malware and distributed denial-of-service (DDOS) attacks and ‘hacking’ incidents. It is proposed to apply in addition to the general data breach notification duty regarding personal data (see above).

**Various DPA investigations in the Internet and social media industry**

In 2014, the DPA investigated various data controllers in the Internet and social media industry. Applications (apps), and the privacy terms of apps, social media services and Internet services were criticized by the DPA in public reports. The DPA also published reports on the use of cookies and profiling.

2. Emerging Privacy Issues and trends

On 28 January 2015, the DPA published the main focus areas of its supervisory and enforcement efforts for 2015. The DPA will particularly look into: (i) profiling, (ii) special (sensitive) personal data, (iii) data processing by
local governmental bodies, (iv) personal data processed in employment relationships and (v) protection of personal data. The DPA has announced it will initiate ‘several investigations’ in the context of these focus areas.

- **Profiling:** the two most important risks connected to profiling are (a) lack in transparency and (b) the danger that decisions are made about people on the basis of an (incorrect) profile. Countering these two risks is one of the key objectives of the DPA in the area of profiling. In addition, in the area of tracking & tracing, the DPA will focus on compliance with the information obligation and whether consent has been obtained in the correct way or an adequate opt-out has been offered.

- **Processing of ‘special’ personal data:** the DPA will specifically focus in 2015 on the processing of health and criminal personal data. With regard to the processing of health data, the DPA identifies three main developments: (1) change of responsibility of care tasks from the State to local governments (municipalities); (2) a trend of large technology companies focusing on the production and promotion of equipment that enables people to self-monitor their health and (3) health care institutions and individual health care practitioners realize insufficiently the necessity to assess and overcome the privacy risks in applying new Information- and Communication Technology.

- **Personal data processed by local governments:** in 2015 the DPA will monitor whether the processing of personal data in the social domain will be in accordance with privacy legislation. Moreover, the DPA will publicize guidelines for the use of camera surveillance in the public domain.

- **Personal data processed in employment relationships:** the DPA will investigate breaches of the DDPA, e.g., the use of camera surveillance for the monitoring of employee performance, the requests for medical data of employees who are under sick leave, etc. The DPA will also encourage compliance through discussions with trade unions and trade associations.

- **Protection of personal data:** the DPA will continue to investigate alleged breaches of the statutory obligation to adequately secure personal data and will make the necessary preparations for efficiently and effectively processing data breach notifications.

**International cooperation**

The DPA is vigorously pursuing international cooperation with other supervisors to enhance the effectiveness of investigating violations of privacy regulations. In addition, the DPA has spent much effort into the revision of the legal framework for data protection in the EU.
3. Applicable Law

The applicable legislation is the Personal Data Protection Act (Wet bescherming persoonsgegevens) of 6 July 2000, implementing the Directive 95/46/EC ("Directive"), as last amended on 26 November 2014 (effective date 1 January 2015) ("PDPA").

Further data protection provisions are included in the Telecommunications Act (Telecommunicatiewet) of 19 October 1998, amongst others, implementing the e-Privacy Directive, as last amended on 26 November 2014 (effective date 11 December 2014) ("TA").

In addition, there are various delegated laws and regulations, the most important of which is the Exemption Decree (Vrijstellingsbesluit Wbp) of 7 May 2001, as last amended on 9 December 2014 (effective date 1 January 2015), which exempts certain processing activities from the notification obligation.

4. Key Privacy Concepts

a. Personal Data

The PDPA applies to the processing of any information ("Personal Data") relating to an identified or identifiable individual/natural person ("Data Subject").

b. Data Processing

"Processing" is extremely broadly defined and covers any operation or set of operations performed on Personal Data including its collection, recording, organization, and deletion. The PDPA applies to automated data processing as well as to manual processing of Personal Data that is entered in a file or intended to be entered therein.

c. Processing by Data Controllers

The PDPA applies to those persons or entities that, alone or in conjunction with others, determine the purpose of and the means for processing Personal Data ("Data Controller"). The PDPA also imposes certain obligations on the Data Processor that processes Personal Data for the Data Controller. The carrying out of processing by a Data Processor shall be governed by an agreement or another legal act whereby an obligation is created between the Data Processor and the Data Controller.

d. Jurisdiction/Territoriality

The PDPA applies to:

- the processing of Personal Data carried out in the context of the activities of an establishment of a Data Controller in the Netherlands; and
• the processing of Personal Data by or for Data Controllers that are not established in the EEA, whereby use is made of automated or non-automated means situated in the Netherlands (unless these means are used only for forwarding Personal Data).

e. **Sensitive Personal Data**

The PDPA prohibits the processing of sensitive Personal Data – that is, Personal Data relating to racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, unlawful or objectionable conduct, criminal conduct, and data concerning health or sexual life. The prohibition on processing of sensitive Personal Data does not apply if the processing is carried out for a specific legitimate purpose provided in the PDPA. Specific exemptions apply for each category of sensitive Personal Data.

Notwithstanding the specific exemptions for the processing of sensitive Personal Data, in general, the prohibition to process sensitive Personal Data does not apply where:

• the processing is carried out with the express consent of the Data Subject (see Section 5(b));

• the Personal Data has manifestly been made public by the Data Subject;

• the processing is necessary for the establishment, exercise, or defense of a right in law;

• the processing is necessary to comply with an obligation of international public law; or

• the processing is necessary with a view to an important public interest, where appropriate guarantees have been put in place to protect individual privacy and this is provided for by law or else the Dutch Data Protection Authority has granted an exemption. When granting an exception, the Data Protection Authority can impose rules and restrictions. Processing sensitive Personal Data on this basis must be notified to the European Commission.

Further exemptions may apply to processing of sensitive Personal Data that is carried out for the purpose of scientific research or statistics (if certain conditions are met).

A number that is required by law for the purposes of identifying a person (e.g., social security number) may only be used for the processing of Personal Data in execution of the said law or for purposes stipulated by the law. Even with the consent of the Data Subject, the processing is prohibited.
f. Employee Personal Data

The PDPA does not provide for specific rules with respect to employees' Personal Data, however employee Personal Data may include both sensitive Personal Data and non-sensitive Personal Data.

Sensitive employee Personal Data may be processed in the circumstances mentioned in Section 4(e). If no specific exemption applies, express consent of the Data Subject will be the most likely justification for processing.

Non-sensitive employee Personal Data may be processed by a Data Controller in certain circumstances, including the performance of the employment contract. A fallback justification for processing both sensitive and non-sensitive Personal Data in the employment context may be if consent is given by the Data Subject. However, there is significant doubt whether consent can be valid in the employment context (see Section 5(d)).

5. Consent

a. General

Consent of the Data Subject is not mandatory, but it is one of the six statutory processing grounds.

While written consent is not required by law, it may be necessary in order to demonstrate that consent has been given unambiguously and/or explicitly. The PDPA does not contain any specific requirements regarding the language of the consent. However, consent should be freely given, specific, and must constitute an informed expression of the Data Subject’s will, which implies that the Data Subject must be informed in a language that he is able to understand. Otherwise, the consent may be deemed invalid.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to only cover the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

In addition, the Data Subject also has the right to withdraw consent at any time.

b. Sensitive Data

Where consent is relied upon to justify the processing of sensitive Personal Data, such consent must be given explicitly prior to the processing. A tacit or implicit consent does not suffice. The Data Subject must have given expression to his or her will to give consent to the specific data processing verbally, in writing or by behavior.
c. **Minors**

For Data Subjects under the age of sixteen, or who have been placed under legal restraint or the care of a mentor, consent of their legal representative(s) must be obtained.

d. **Employee Consent**

The general rule is that employee consent is required to collect and process an employee’s Personal Data; however, there are instances when employee consent is not required, e.g., to carry out an employment contract or administer an employment relationship, or to fulfill a legitimate interest of the employer.

e. **Online/Electronic Consent**

In the Netherlands, online or electronic consent is permissible and deemed effective if properly structured and evidenced.

6. **Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; how to contact the privacy officer or other person accountable for the organization's policies and practices; how to make an inquiry or file a complaint; how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

7. **Processing Rules**

An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. **Rights of Individuals**

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.
9. Registration/Notification Requirements

Though not mandatory, an organization that collects and processes Personal Data may be required to notify the appropriate data authority.

Please note the Exemption Decree (Vrijstellingsbesluit Wbp) of 7 May 2001, as last amended on 5 May 2012, which exempts certain processing activities from the notification obligation.

10. Data Protection Officers

In the Netherlands, there is no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

Transfers of Personal Data from the Netherlands to countries within the EEA and Canada, Switzerland, Guernsey, the Isle of Man, Argentina, Israel and to US recipients which have signed up under the Safe Harbor arrangement, are generally permitted without the need for further approval.

Cross-border transfers of Personal Data to a country that does not offer an adequate level of protection, may take place provided:

- the Data Subject has unambiguously consented to the transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller, or for actions to be carried out at the request of the Data Subject and that are necessary for the conclusion of a contract;
- the transfer is necessary for the conclusion or performance of a contract concluded between the Data Controller and third parties in the interests of the Data Subject;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims;
- the transfer is necessary in order to protect the vital interests of the Data Subject;
- the transfer is carried out from a public register set up by law or from a register that can be consulted by anyone or by any persons who can invoke a legitimate interest; or
- an (unaltered) Model Contract within the meaning of Article 26 par. 4 of the Directive 95/46/EC is used.
If the above legal grounds for cross-border data transfer do not apply, the cross-border data transfer to a non-EEA country with an inadequate level of protection may be authorized by the Dutch Minister of Security and Justice. Thus, the Data Controllers, on the basis of a data transfer agreement and after consultation with the Dutch Data Protection Authority, must obtain a permit from the Dutch Minister of Security and Justice with regard to the data transfer. The Dutch Data Protection Authority must be notified of and must approve any data transfer agreement in advance.

12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

In 2013, the DPA issued guidance on this topic. According to these guidelines, organizations should first conduct a risk analysis to determine the desired level of security. Secondly, organizations are advised to adhere to “generally accepted security standards”, for example the Code for Information Security (“Code voor Informatiebeveiliging”). The guidelines further state that organizations should conduct an evaluation of their systems on a regular basis.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors. In case of an occurrence of data breach, the outsourcing organization may be held liable together with the third party provider.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
The Netherlands has implemented data breach notification obligations set out in Articles 4(3) and 4(4) of the e-Privacy Directive in Article 11.3a of the Telecommunications Act (TA). In case of a data security breach with detrimental effects for the protection of Personal Data, the TA imposes an obligation on providers of public electronic communication services to notify the Authority Consumers and Markets (ACM) as soon as possible. In addition,
the provider must notify the relevant Data Subjects if their Personal Data is at risk. If the provider fails to notify the Data Subjects, the ACM may order the provider to do so.

While currently, the notification obligation only applies to providers of public electronic communications services, a legislative bill introducing a general data breach obligation will become effective on 1 January 2016 (see Section 1).

An organization that is involved in a data breach situation may be subject to a suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, or civil actions and/or class actions, or a criminal prosecution.

16. Accountability

Subject to regulatory guidance, organizations may be required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data; furnish the results of the privacy impact assessments to privacy regulators upon request; and furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

17. Whistle-blower hotline

Whistle-blower hotlines may be established in the Netherlands provided that they are in compliance with local laws, and that appropriate filings have been made with the data authority.

18. E-discovery

When implementing an e-discovery system, an organization is required to advise employees of the implementation of an e-discovery system, the monitoring of work tools, and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace, and give employees the opportunity to review the isolated emails designated as spam.

20. Cookies

The Netherlands has implemented the rules regarding cookies and similar techniques set out in Article 5 (e) of the e-Privacy Directive in Article 11.7a of the Telecommunications Act.

Anyone who wishes to store information, or gain access to information already stored, in the terminal equipment of a user, may only do so after the user is provided with clear and complete information, and after the user has given his
consent. There are exceptions to this rule. Prior information and consent are not required if, and to the extent that, storing information or gaining access to information is strictly necessary for (a) carrying out the transmission of communication over an electronic communications network; (b) to provide a user with an information society service, which has been explicitly requested; or (c) to obtain information about the quality or effectiveness of a delivered service of the information society, provided that it has no or little impact on the privacy of the subscriber or user concerned (i.e. for analytical cookies with a low privacy impact).

The Minister of Justice and the relevant authorities have given extensive guidance on the consent and information requirements. Implied consent can, in some circumstances, be relied upon. For example, a banner stipulating which cookies are used, with a reference to a complete information document, and indicating that consent is implied if a user continues using the website, has been considered sufficient to obtain consent.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.
New Zealand

Carl Blake
Auckland
Tel: +64 9 977 5163
carl.blake@simpsongrierson.com

Karen Ngan
Auckland
Tel: +64 9 977 5080
karen.ngan@simpsongrierson.com
1. Recent Privacy Developments

The key legislation governing privacy in New Zealand is the Privacy Act 1993 ("Privacy Act"). The Privacy Act sets out a number of Information Privacy Principles ("IPPs") that govern the collection, storage and security, accuracy, retention, use and disclosure of personal information. The Privacy Act applies to "agencies", including Government, private sector businesses, voluntary sector and non-government organisations.\(^1\) In 2011, the Law Commission completed a comprehensive four-stage review into the Privacy Act, issuing a report setting out a number of recommended changes to the Privacy Act.\(^2\)

A number of the Law Commission’s recommendations have been adopted as part of the Government’s interim response to the report including the adoption of provisions allowing the sharing of personal information to facilitate the provision of public services.\(^3\) In March 2014, the Cabinet Social Policy Committee released a paper setting out a proposal for the adoption of a new Privacy Act to address the remaining Law Commission recommendations that the Government proposes to adopt ("Cabinet Paper").\(^4\) A draft Privacy Bill has yet to be released but based on the Cabinet Paper the substantive issues expected to be addressed include:

- mandatory breach notification;
- the issue of compliance notices for Privacy Act breaches;
- strengthened own motion investigations by the Privacy Commissioner and increased fines;
- cross border outsourcing, disclosures and enforcement co-operation; and
- streamlining the complaints procedure.

2. Emerging Privacy Issues and Trends

(a) **Mandatory data breach notification**: Currently, there are no provisions requiring agencies to notify subjects when a privacy breach has occurred. However, the Cabinet Paper indicates that a two tier approach may be adopted for privacy breaches:

(i) Tier 1 – material breaches, which are to be notified to the Privacy Commissioner; and

---

\(^1\) Privacy Act 1993, s 2. There are a number of limited exceptions including the Sovereign, Governor-General, a court or tribunal in carrying out its judicial functions, an ombudsman or commission of inquiry and a news medium in relation to its new activities.
\(^3\) Privacy Amendment Act 2013.
\(^4\) Cabinet Social Policy Committee “Reforming the Privacy Act 1993” (13 March 2014).
(ii) Tier 2 – more serious breaches, which are to be notified to the Privacy Commissioner and to the affected individuals;

The Privacy Commissioner has also recently issued a “name and shame” policy under which it is proposing to name agencies who are in breach of the Privacy Act. See section 15 for further discussion on data breach notification and the current guidelines in place.

(b) Cross-border Outsourcing and Disclosures: When a New Zealand agency offshores personal information and engages an overseas provider for storage or processing, the New Zealand agency generally remains responsible and accountable for that data. However, this is not necessarily the case where the offshore provider uses or processes the information for that provider’s own purposes. The Cabinet Paper indicates the intent to adopt a new IPP, making it clear that New Zealand agencies remain accountable for what happens to information outsourced to an overseas provider. There is also an intent to adopt a new IPP that requires New Zealand agencies to take reasonable steps to ensure that information disclosed overseas will be subject to acceptable privacy standards in the foreign country.

(c) APEC Cross-Border Privacy Rules: The Government has indicated it will undertake work to determine whether the APEC cross-border privacy system may provide a mechanism to increase benefits or reduce compliance costs.

(d) Regulation of Drones: The Civil Aviation Authority has launched new civil aviation rules for the operation of drones which came into force on 1 August 2015. The new rules deal with safety and some of the privacy issues raised by drones. The new rules include a requirement that drone operators get permission from property owners before they may fly their drone overhead and have the consent of anyone they want to fly over. The New Zealand Privacy Commissioner has also commented on the use of drones and the requirement that drone operators comply with the Privacy Act, the same as users of any camera, including mobile phones or automated CCTV systems.

3. Law Applicable

(a) Privacy Code: As noted above, the key legislation dealing with privacy in New Zealand is the Privacy Act. The long title states the general object of the Privacy Act is to “promote and protect individual privacy”. Although the IPPs are not enforceable in a court of law, a breach can become the subject of a complaint to the Privacy Commissioner and possibly the
Human Rights Review Tribunal ("HRRT"). The functions of the Privacy Commissioner include auditing personal information maintained by an agency, monitoring the use of unique identifiers and compliance with the IPPs.

(b) Privacy Codes of Practice: Part 6 of the Act allows the Privacy Commissioner to issue codes of practice which apply the IPPs within particular industries, sectors or context ("Privacy Code"). A Privacy Code may modify the application of any of the IPPs, for example, by prescribing standards that are more stringent, or less stringent, than the standards prescribed under the Act. A Privacy Code can be issued in respect of specified information or classes of information, specified agencies or classes of agency, an industry or profession or class of industries or professions.

(c) Savings: The Privacy Act interacts with a number of other statutes and laws, and section 7 of the Privacy Act sets out a number of exceptions to the application of certain IPPs.

4. Key Privacy Concepts

a. Personal Data

Personal information is defined as “information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages an Relationships Registration Act 1995”. The term “individual” is defined to mean “a natural person, other than a deceased natural person”.

b. Data Processing and Processing by Data Controllers

There are no specific references to data processing or processing by data controllers in the Privacy Act. Generally personal information should only be processed if that is one of the purposes for which the information was collected (or a directly related purpose). Section 3(4) of the Privacy Act states that where an agency holds information solely as an agent, for the sole purpose of safe custody, or for the sole purpose of processing the information, on behalf of another agency, and does not process the information for its own purposes, the information shall be deemed to be held by the agency on whose behalf that the information is so held.

---

7 Privacy Act, s 11.
8 Privacy Act, s 13(1).
9 Privacy Act, s 46.
10 Privacy Act, s 2(1).
11 An exception to this is health information in certain circumstances – see Privacy Act s 46(6)(a).
c. Jurisdiction/Territoriality
The Privacy Act does not purport to have extraterritorial effect on persons outside of New Zealand, but section 10 of the Privacy Act does provide that the IPPs relating to storage and security, accuracy, retention, use and disclosure of information held by an agency includes information that is held outside New Zealand by that agency, where that information has been transferred out of New Zealand by that, or any other agency. In addition, for the purposes of the IPPs relating to access to and correction of information, information held by an agency includes information held outside New Zealand by that agency.

d. Sensitive Personal Data
There are no specific references in the Privacy Act to Sensitive Personal Data.

e. Employee Personal Data
There are no specific references in the Privacy Act to Employee Personal Data, although various information an employer collects, uses and discloses about its employees in the ordinary course of business will likely constitute personal information under that Act.

One of the key exceptions available to an agency to refuse a request for personal information under the Privacy Act is predominantly relevant in an employment context. An agency may refuse disclosure of personal information if it would breach a promise of confidentiality given in respect of the supply of “evaluative material”. Three tests must be met in order for the evaluative material exception to apply:

(a) the requested information must be “evaluative material”, which is defined as including material compiled solely for the purpose of determining an individual’s suitability, eligibility or qualifications for employment;

(b) its disclosure must breach an express or implied promise of confidentiality, and

(c) the information in question must have been “supplied” from a third party and the promise of confidentiality must be owed to the supplier (for example a job reference from a former employer).

5. Consent

a. General
There is no express requirement for an agency to obtain an individual’s express consent to collect personal information. However, personal information should generally be collected directly from the individual concerned and when personal information is collected directly from that individual, the agency collecting the information should take reasonable steps to ensure that individual is aware of certain matters, including the purpose for
which the information is being collected. There are a number of exceptions to
these general principles, including collecting personal information from a
person other than the individual concerned if authorised by the individual
concerned. Personal information may also be used for a purpose other than
that for which it was collected if authorised by the individual concerned.

b. Sensitive Data
There are no specific provisions in the Privacy Act regarding sensitive data.

c. Minors
The Privacy Act and IPPs do not specifically distinguish between adults and
children in relation to consent. The Law Commission has made
recommendations to amend IPP4 (manner of collection of personal
information) to provide that, in considering whether the collection of personal
information is unfair or unreasonably intrusive, the age of the individual
concerned must be taken into account.\(^{12}\)

d. Employee Consent
There are no provisions in the Privacy Act regarding employee consent,
except in so far as to provide that an employer may use or disclose personal
information for various reasons, including where authorisation has been
provided for such use/disclosure. Privacy in the workplace must also be
considered in the context of the special nature of the employment relationship.
The Employment Relations Act 2000 provides a comprehensive framework for
the employment relationship and imposes mutual obligations of trust,
confidence and good faith.\(^{13}\) No specific recommendations have been made
by the Law Commission as of yet in relation to the Privacy Act.\(^{14}\)

e. Online or Electronic consent
There is no specific provision in the Privacy Act regarding online or electronic
consent to disclosure of personal information. However, online privacy policies
and terms are generally considered effective if appropriately structured and
accessible.

6. Information/Notice Requirements
IPP3 (collection of information from subject) governs the notice requirements
an agency must comply with when that agency is collecting personal
information. An agency is required to take such steps (if any) as are in the
circumstances, reasonable to ensure that the individual concerned is aware
of, amongst other things, the purpose for which the information is being
collected and the intended recipients of that information.

\(^{12}\) Law Commission, above n 2, at 307.
\(^{13}\) Employment Relations Act 2000, s 3.
\(^{14}\) At 313.
7. Processing Rules

The use of personal information, is covered under IPP10 (limits on use of personal information). This principle holds that an agency which obtains personal information for a particular purpose shall not use that information for any other purpose. There are a number of exceptions to this rule, such as where the agency reasonably believes that the source of the information is publicly available or there is authorisation from the individual concerned.

IPP5 governs the storage and security of personal information. Under this principle, an agency shall ensure that the information is protected against loss, access, use, modification, disclosure (except with the authority of the agency that holds the information) or other misuse. See also Section 13 below.

8. Rights of individuals

Information subjects, or the individual of whom the information is concerned, have various rights under IPP6 (access to personal information) and IPP7 (correction of personal information). Under IPP6, the individual concerned shall be entitled to obtain confirmation that their personal information is being held, and to have access to that information. Under IPP7, the individual concerned shall be entitled to request correction of their information, and if the correction is not made, to request that there be attached to the information a statement of the correction sought but not made.

9. Registration/Notification requirements

There are currently no registration or notification requirements under the Privacy Act.

10. Data Protection Officers

In New Zealand, it is the responsibility of each agency to ensure that there are one or more Privacy Officers whose responsibilities include encouraging compliance with the IPPs and the Privacy Act, working with the Privacy Commissioner in relation to investigations conducted pursuant to Part 8 of the Privacy Act, and dealing with privacy requests.

11. International Data Transfers

As mentioned above, Section 10 of the Privacy Act applies some of the IPPs to personal information transferred or held by an agency overseas.\(^\text{15}\) In addition under part 11A of the Privacy Act, the Privacy Commissioner may prohibit a transfer of personal information from New Zealand (by a transfer

\(^{15}\) See above “Key Privacy Concepts: Jurisdiction/Territoriality”.

Baker & McKenzie
prohibition notice)\textsuperscript{16} to another State if the Privacy Commissioner is satisfied, on reasonable grounds, that

(a) the information has been, or will be received in New Zealand from another state and is likely to be transferred to a third state that will not be subject to a law providing comparable safeguards to the Privacy Act; or

(b) that the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines and set out in Schedule 5A of the Privacy Act.\textsuperscript{17}

12. Security Requirements

Under IPP5, an agency that holds personal information is required to ensure that the information is protected, by reasonable security safeguards, against loss, access, use, modification, disclosure and other misuse.\textsuperscript{18}

13. Special Rules for the Outsourcing of Data Processing to Third Parties

IPP5 also provides that where it is necessary for personal information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of that information.\textsuperscript{19} Where that third party holds that information solely as agent or the sole purpose of safe custody or processing on behalf of an agency, and the information is not used or disclosed for that third party’s own purposes, the information is deemed to be held by the agency on whose behalf the information is so held or processed.

14. Enforcement and Sanctions

Any person may make a complaint to the Privacy Commissioner alleging that any action is, or appears to be, an interference with the privacy of an individual. An action is an interference with the privacy of an individual if:

(a) in relation to that individual:

(i) the action breaches an IPP; or

(ii) the action breaches a code of practice; or

(iii) the action breaches an IPP or code of practice as modified by an Order in Council; or

(iv) the provisions of an information sharing agreement approved by an Order in Council have not been complied with; or

\textsuperscript{16} Privacy Act, s 114D.
\textsuperscript{17} Privacy Act, s 114B.
\textsuperscript{18} IPP 5.
\textsuperscript{19} IPP 5.
(v) the provisions of Part 10 (information matching) have not been complied with; and

(b) the Privacy Commissioner is satisfied that the action:

(i) caused, or may cause loss, detriment, damage, or injury to that individual; or

(ii) has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of that individual; or

(iii) has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of that individual.  

On receipt of a complaint the Privacy Commissioner may investigate, or elect to take no further action. The Privacy Commissioner may also refer a complaint to an Ombudsman, the Health and Disability Commissioner, the Inspector General of Intelligence and Security or to an overseas privacy enforcement authority if the Privacy Commissioner determines that such persons or authority should deal with the complaint. If an investigation is undertaken by the Privacy Commissioner, the Privacy Commissioner is required to conduct the investigation with due expediency and is also required to inform the parties of the result of that investigation.

If the Privacy Commissioner believes it is possible to secure a settlement to a complaint or otherwise considers, following an investigation, that a complaint has substance, the Privacy Commissioner will use best endeavours to secure a settlement and if appropriate, an assurance against repetition. If a settlement cannot be reached the matter may be referred to the Director of Human Rights Proceedings who may choose to issue proceedings before the HRRT. The aggrieved individual may also issue proceedings before the HRRT if the Director of Human Rights Proceedings does not do so.

The remedies, if a breach of privacy is found by either the HRRT, can include one or more of the following:

- a declaration;
- an order restraining the defendant from continuing or repeating the interference;
- damages;

---

20 Privacy Act, s 66.
21 Privacy Act, s 71.
22 Privacy Act, s 75.
23 Privacy Act, s 82.
24 Privacy Act, s 83.
25 Privacy Act, s 85.
• an order requiring the defendant to perform specified acts with a view to remedying the interference, or redressing any loss or damage suffered by the aggrieved individual; or

• such other relief as the HRRT thinks fit.

15. Data Security Breach

Currently, there are no legal obligations on agencies to notify individuals that their personal information has been lost or accessed improperly. However, the Privacy Commissioner has issued guidelines on good practice in such a situation. These guidelines are intended to assist agencies plan in advance for a breach to ensure that they are prepared to manage breaches successfully, for the benefit of the agency and affected individuals.26 Under these guidelines, those affected by a privacy breach should be notified, as prompt notification can assist with loss mitigation. Agencies are also encouraged, under the guidelines, to notify the Office of the Privacy Commissioner (“OPC”) of material privacy breaches. Further, in support of data security breaches, the OPC released a “name and shame” policy where agencies may be publicly named for a number of reasons, including matters uncovered in the monitoring of information sharing agreements or following self-notification of a breach.27 Agencies will only be named where, on balance, the Privacy Commissioner considers that the agency ought to be named for the purpose of giving effect to the Privacy Act.

16. Accountability

There are currently no mandated requirements for compliance with the Privacy Act. The current Privacy Act is based largely on the principle of allowing agencies flexibility to apply the Privacy Act in a way that best fits their circumstances.28 Section 13(1)(b) of the Privacy Act allows the Privacy Commissioner to conduct a private audit of an agency if that agency requests it. While the Law Commission has recommended that the Privacy Commissioner be granted the power to conduct compulsory audits where there are good reasons, the Government has indicated it will instead enhance the Privacy Commissioner’s own motion investigation powers and increase the penalties for failing to comply with an information report from the Privacy Commissioner.29

26 Privacy Commissioner Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist (February, 2008).
28 Cabinet Social Policy Committee, above n 4, at 3.
29 Cabinet Social Policy Committee, above n 4, at 8.
17. Whistle-blower Hotline

Whistle-blower hotlines may be implemented in New Zealand provided they comply with the Privacy Act (and other applicable employment statutes).

The Protected Disclosures Act 2000 (“PDA”) facilitates the disclosure and investigation of matters of “serious wrongdoing” in or by an organization. The PDA protects employees who, in accordance with the PDA, make disclosures about serious wrongdoing, including unlawful or corrupt practices. The PDA does not specifically relate to personal information under the Privacy Act, but does raise issues under that Act where complaints are made about individuals within an organisation. Organisations must apply the principles of the Privacy Act when investigating disclosures about serious wrongdoing.

Section 19(1) of the PDA provides that every person to whom a protected disclosure is made or referred must use his or her best endeavours not to disclose information that might identify the person who made the protected disclosure unless:

(a) that person consents in writing to the disclosure of that information; or

(b) the person who has acquired knowledge of the protected disclosure reasonably believes that disclosure of identifying information:

(i) is essential to the effective investigation of the allegations in the protected disclosure; or

(ii) is essential to prevent serious risk to public health or public safety or the environment; or

(iii) is essential having regard to the principles of natural justice.

18. E-Discovery

There are currently no express or unique requirements for compliance with the Privacy Act during an E-Discovery process. However, various principles of the Privacy Act will apply to any discovery process where proceedings have been commenced or are reasonably in contemplation:

- IPP2 allows non-compliance with the requirement for an agency to collect the information directly from the individual concerned where it believes, on reasonable grounds, that non-compliance is necessary for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation);

- IPP10 allows non-compliance with the requirement for an agency that holds personal information that was obtained in connection with one purpose not to use the information for any other purpose where it believes, on reasonable grounds, that non-compliance is necessary for the conduct of proceedings before any court or tribunal (being
proceedings that have been commenced or are reasonably in contemplation); and

- IPP10 allows non-compliance with the requirement for an agency that holds personal information not to disclose the information to others where it believes, on reasonable grounds, that non-compliance is necessary for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation);

19. Anti-Spam Filtering

There are currently no express or unique requirements for compliance with the Privacy Act in relation to anti-spam filtering. As a matter of best practice, any anti-spam filtering policy should be documented within an agency’s code of conduct or employee handbook/policies and properly notified to employees.

20. Cookies

There are no specific laws or rules regulating the use and deployment of cookies in New Zealand, however agencies must comply with IPP2 (source of personal information) and therefore authorisation from the individual must be obtained before cookies can be used in relation to the collection of personal information.

21. Direct Marketing

Whether or not personal information can be used for direct marketing purposes will depend on whether this is one of the purposes for which the personal information was collected. Some exceptions to this include where the information is publicly available, the individual concerned has authorised use of the information for this purpose or such use directly related to the purpose for which it was collected. Where marketing material is sent by electronic means (e.g., email, instant message, text message or fax), the Unsolicited Electronic Messages Act 2007 ("Anti-Spam Act") will be applicable. The Anti-Spam Act prohibits the sending of unsolicited commercial electronic messages, being a commercial electronic message which the recipient has not consented to receiving.
Norway

Espen Sandvik
Oslo
Tel: +47 98 29 45 41
esa@adeb.no
1. Recent Privacy Developments

Implementation of Data Retention Directive cancelled

The Norwegian Parliament adopted the Data Retention Directive (2006/24/EC) in 2011. However, the implementation of the Directive was not yet in force when the Court of Justice of the European Union on 8 April 2014 declared the Directive invalid (joined cases C-293/12 and C-594/12). Shortly afterwards, the Norwegian Minister of Communication declared that the implementation would be put on hold. The Prime Minister has subsequently announced that there is a need for a certain retention of traffic data, and that adopting purely domestic laws could be an option. There is not yet any proposal for such new laws.

Right to be forgotten – in Norway

The landmark decision by the Court of Justice of the European Union in the “right to be forgotten” case (C-131/12), provides the right for data subjects to demand that search engine operators remove search results with links to third party websites featuring certain personal data. The criteria is that the information in question is inaccurate, inadequate, irrelevant or excessive. Even if the Court’s decision is not binding for Norway as a non-EU member, it is in practice seen as giving decisive guidance on Norwegian data privacy law in this area, as Norwegian law is based on the implementation of Directive 95/46/EC. The Data Inspectorate handles complaints in cases where there is a rejection of removal requests. So far, the only removal request that the Data Inspectorate has accommodated concerned websites featuring allegations of doping against an athlete, and where the websites in question did not contain the information that the data subject was later acquitted.

Transfer of data abroad made easier

The personal data Regulation was amended with effect from 1 July 2014, in order to allow the transfer of data abroad to data processors in third countries without adequate data protection. This can be done provided that the EU model contract for such transfers have been entered into, and the Data Inspectorate has been notified in advance.

Insurance companies’ hidden video surveillance allowed

In a decision from the Borgarting Court of Appeal in April 2014, an insurance company was found not to have violated the Personal Data Act by the secret surveillance and videotaping of an insurance policy holder. The data subject in question had filed a claim for insurance payment based on disability. The insurance company had reasons to believe that the individual did not suffer from such disability as was basis for the claim. As the insurance company had no other way of proving this in the specific case, the Court found that the secret surveillance and videotaping in question was allowed. The same
conclusion was reached in a similar case before the Privacy Protection Committee later the same year.

**Data Inspectorate opposes sale of top domains for data privacy reasons**

Norway has three top domains, .no (for Norway), .sj (for Svalbard and Jan Mayen) and .bv (for the Bouvet Island), but only the .no domain is currently open for use. A proposal to lease the .bv top domain to the Netherlands triggered a joint protest letter to the Minister of Communication from the Data Inspectorate, the Consumer Council and the Technology Board. One of the reasons for the protest was that the top domains in question could instead be used for secure Internet zones, the use of which would be subject to particular restrictions and demands with respect to data privacy and use of cookies. No decision has yet been made.

**Police Register Act in force**

The Police Register Act was adopted in 2010, and eventually entered into force on 1 July 2014. The Act aims to ensure that information security and data privacy are safeguarded when the police process personal data. The Act establishes several requirements to police registers, and also provides rights to the data subjects such as the right of access.

**New Health Register Act and Patient Journal Act**

The old Health Register Act has been replaced by the New Health Register Act and the Patient Journal Act effective 1 January 2015. The new Health Register Act governs the use of personal health data for research and quality assurance, whereas the Patient Journal Act governs the use of personal health data for medical treatment. The new legislation governs, amongst others, who may access health data and what it may be used for, and provides the right for patients to know who has accessed their personal health data. The Data Inspectorate has said that the privacy consequences of the new legislation are debatable, in particular due to the possibility to transfer health data to other health organizations.

2. **Emerging Privacy Issues and Trends**

**General Data Protection Regulation**

The EU’s European Council aims for adoption of the new General Data Protection Regulation in late 2015. It is expected that Norway will implement the Regulation on the basis of the EEA agreement.

**Anti-terrorism measures proposed**

The government has announced that it will propose a new “package” of anti-terrorism measures in 2015, and it is expected that this will authorize the Police Security Service (“PST”) to use a number of surveillance tools that raise data privacy issues. The PST submitted a proposal in August 2014 for
the right to collect and use “big data” in order to identify relevant trends and challenges, which was rejected. The striking of the balance between protecting data privacy and ensuring security will undoubtedly raise discussions in light of recent events. These events include both on the one hand the recent terrorism attacks in France and reports of increased risk of terrorism in Norway, and on the other hand the recent detection in Norway of illegal espionage on data and voice traffic by the use of so-called IMSI-catchers acting as false base stations, and other disclosures of foreign surveillance of Norwegian individuals.

3. Law Applicable

The general regulation of personal data is found in the Personal Data Act 2000 (lov LOV-2000-04-14-31) as amended, and the sub-ordinate Personal Data Regulation 2000 (FOR-2000-12-15-1265), which implement the Data Protection Directive (95/46/EC). Further provisions relevant to data privacy are found in the following Acts, among others:

- The Marketing Act 2009 (LOV-2009-01-09-2), which restricts direct marketing.
- The Health Register Act 2014 (LOV-2014-06-20-43), which governs the use of personal health data for research and quality assurance.
- The Health Research Act 2008 (LOV-2008-06-20-44), which governs the use of personal data for health research purposes.
- The Police Register Act 2010 (LOV-2010-05-28-16), which governs the police’ processing of personal data.

4. Key Privacy Concepts

a. Personal Data

The Personal Data Act defines “personal data” as “any information and assessments that may be linked to a natural person”.

b. Data Processing

“Processing of personal data” is defined as “any use of personal data, such as collection, recording, alignment, storage and disclosure or a combination of such uses”. The Personal Data Act applies to a) all processing of personal data wholly or partly by electronic means, b) other processing of personal data
c. Processing by Data Controllers
The Personal Data Act applies to those persons who determine the purpose of the processing of personal data and the means to be used (“data controller”).

d. Jurisdiction/Territoriality
The Personal Data Act applies to data processing activities carried out by:

- Data controllers established in Norway; and
- Data controllers that are not established in the EEA but that use equipment located in Norway to carry out data processing activities (other than merely for the purpose of transit).

e. Sensitive personal data
The Personal Data Act imposes additional requirements for the processing of sensitive personal data – that is, personal data relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health or condition, sexual life, commission or alleged commission of any offense, or criminal proceedings. Specifically, the processing of sensitive personal data is prohibited unless one of a number of stated conditions is met. These include:

a) the data subject consents to the processing,
b) there is statutory authority for the processing,
c) the processing is necessary to protect the vital interests of a person, and the data subject is incapable of giving his or her consent,
d) the processing relates exclusively to data which the data subject has voluntarily and manifestly made public,
e) the processing is necessary for the establishment, exercise or defence of a legal claim,
f) the processing is necessary to enable the controller to fulfil his obligations or exercise his rights in the field of employment law,
g) the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where the data are processed by health professionals subject to the obligation of professional secrecy, or
h) the processing is necessary for historical, statistical or scientific purposes, and the public interest in such processing being carried out clearly exceeds the disadvantages it might entail for the natural person.
Non-profit associations and foundations may process sensitive personal data in the course of their activities even if such processing does not satisfy one of the conditions above. Such processing may apply solely to data relating to members or to persons who, on account of the purposes of the association or foundation, voluntarily have regular contact with it, and solely to data which are collected through such contact. The personal data may not be disclosed without the consent of the data subject. The Data Inspectorate may decide that sensitive personal data may also be processed in other cases if this is warranted by important public interests and steps are taken to protect the interests of the data subject.

**f. Employee personal data**

Employee personal data is likely to include both non-sensitive personal data and sensitive personal data (e.g., health-related information). Sensitive employee personal data may be processed under the circumstances mentioned in Section 4(e) above, commonly for the purpose of carrying out the data controller’s obligations in the field of employment law. Non-sensitive employee personal data may be processed by a data controller for purposes that are necessary in order to maintain and administer the employment relationship (e.g., performance of a contract to which the data subject is a party, or carrying out the data controller’s legal obligations). Other justifications for processing non-sensitive employee personal data may include purposes which are of legitimate interest to the data controller and which are considered to be of greater weight than the data subject’s interest in his or her protection of the personal integrity. A fall-back justification for processing both sensitive and non-sensitive personal data in the employment context may be if consent is provided by the data subject. However, there are limitations on what is considered to constitute valid consent in the employment context (see Section 5(d) below).

5. **Consent**

a. **General**

Consent of the data subject will constitute a sufficient legal ground for the processing of personal data. The processing of personal data may also be allowed on other grounds and without consent, as further defined in the Personal Data Act. The consent must be voluntary, informed and explicit. Written consent is not required. Consent can be revoked at any time.

b. **Sensitive Data**

Consent of the data subject will constitute a sufficient legal basis for the processing of sensitive data, but such processing may in some cases be allowed on other grounds. The requirements to consent are in principle the same for the processing of sensitive data, as for non-sensitive data, but the application of these principles will in practice be somewhat stricter.
c. Minors

The Personal Data Act does not specify a minimum age at which a child can provide valid consent. The Data Inspectorate has however together with the Consumer Ombudsman provided guidelines, according to which data subjects can consent themselves from the age of 15. Children below 15 may only consent to the processing of their personal data in connection with minor competitions and similar arrangements, where the data is used for the purpose of contacting prize winners. In case the consent relates to the processing of sensitive data, the data subject must be 18 in order to consent. For data subjects not having reached the required age, the parents can consent on their behalf. Children are however entitled to revoke a consent given by their parents. To the extent that minors are allowed to consent themselves, the requirement to the consent being “informed”, means that the information in question must be adapted so that it will be understood by the minor.

d. Employee Consent

In Norway, there are doubts as to when consent given in the context of an employment relationship can be considered valid. It will often be questionable whether consent would qualify as voluntary, given that the employee may feel forced to consent due to the subordinate nature of their relationship with their employer. It is however assumed that employee consent in some cases can be seen as voluntary and valid, as the Personal Data Regulation § 7-16 expressly give effect to consent from employees.

e. Online/Electronic Consent

Online or electronic consent is permissible and deemed effective if properly structured and evidenced.

6. Notice Requirements

An organization that collects personal data directly from the data subject, must provide the data subject with information on: the name and address of the data controller and its representative (if any); the purposes for which the data is intended to be processed; whether or not the data will be transferred to a third party, and if so to whom; that it is voluntary for the data subject to provide the data; and other information as required for the data subject to be able to enforce his/her rights in the best possible manner, including the statutory right to access and rectify data.

Where data is obtained from a third party, the data controller will have to provide the data subject with the same information as referred to in the paragraph above, unless the collection of data in question has an express legal basis, notification is impossible or disproportionately difficult, or it is clear that the data subject already is aware of the information and could potentially have been notified.
7. Processing Rules

An organization that processes personal data must limit the use of personal data to only those activities which are necessary to fulfill the identified purpose(s) for which the personal data was collected; and delete or anonymize personal data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data subjects have the general right to: be informed by an organization of the personal data the organization holds about the data subject and how the data subject’s personal data is being processed; access the data subject’s personal data subject to some restrictions and/or qualifications; request the correction of the data subject’s personal data; and request the deletion and/or destruction of the data subject’s personal data.

9. Registration/Notification Requirements

All electronic processing of personal data is, as a starting point, subject to notification to the Data Inspectorate. A notification is required for each category of data processing, meaning that one data controller may have to submit several notifications. The notifications must be filed no later than 30 days before the processing begins, and must be renewed every three years. Standard online filing forms can be used, and the information required is limited. The processing of sensitive data is subject to an authorization from the Data Inspectorate. A number of exceptions are found from these notification obligations and authorization requirements. For instance, certain categories of data such as employee data and customer data are exempted, provided certain conditions are met.

10. Data Protection Officers

In Norway, there is no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

Transfers of personal data from the UK to EEA Member States are generally permitted without the need for further approval. Transfers are also permitted to Canada, Argentina, Guernsey, the Isle of Man, Jersey, the Faroe Islands, Andorra, Israel, Switzerland, New Zealand and Uruguay, which are the subject of the European Commission’s findings of adequacy (subject to the fulfillment of certain pre-conditions) in relation to their data protection laws. Transfer to the US is permitted where the recipient has signed up to the Safe Harbor arrangement.
Subject to the specific authorizations mentioned above, personal data may not be transferred to countries outside the EEA. Exceptions to this general prohibition are, however, expressly contemplated under the DP Act, including where:

- the data subject has consented to the transfer;
- the transfer is necessary to perform a contract with the data subject, or to take steps at his request with a view to entering into a contract with him;
- the transfer is necessary for the conclusion or performance of a contract entered into between the data controller and third parties in the interests of, or at the request of, the data subject;
- the transfer is necessary to protect the vital interests of the individual, or for reasons of public interest, or in connection with legal proceedings, or for the purpose of obtaining legal advice or establishing, exercising or defending legal rights; or
- the transfer has been specifically authorized by the Data Inspectorate.

The adoption of model contractual clauses approved by the European Commission will also provide an adequate level of protection to justify the transfer. Note that the data controller must, in any event, justify all of its data processing under the Personal Data Act; justification of any transfers is an additional compliance requirement. The transfer contract must be filed with the Data Inspectorate before the transfer takes place.

Where multinational organizations are transferring personal information outside the EEA, but within their group of companies, they may also adopt binding corporate rules ("BCR") as a means of justifying such intra-group transfers. Acceptable BCRs may include intra-group agreements, policies or procedures, and special arrangements among the group of companies that afford the requisite protection. The Data Inspectorate, along with the other DPAs across the EEA have agreed to mutually recognize BCRs approved by one of these DPAs. For BCRs to enable the transfer of personal information freely within a corporate group, they must be approved by at least one DPA that has agreed to mutually recognize BCR applications, and by any remaining DPAs in EEA countries from which the organization transfers personal data and which have not agreed to mutual recognition of BCR applications. The Article 29 Working Party has adopted a model checklist and a table setting out the required contents of an application to a data protection authority for approval of a proposed BCR.
12. Security Requirements

Organizations are required to take steps to ensure that personal data in its possession and control are protected from unauthorized access and use. Appropriate physical, technical and organization security safeguards to protect personal data must be implemented, and the organization must be able to document such safeguards. The level of security must be in line with the amount, nature, and sensitivity of the personal data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

A transfer of personal data must as a general rule be necessary for the purpose of the processing. Organizational, cost efficiency, and security reasons are normally viewed as acceptable reasons for a transfer of personal data due to outsourcing. Although the personal data processing is outsourced, the controller remains responsible for the processing activities. Consequently, the controller must make sure that the provisions under the data processing agreement and other related regulations are complied with, both by the controller and the third party service provider. The third party service provider and its sub processors (if any) are viewed as data processors. It is a statutory requirement that a written contract is entered into with the data processor (see Section 7 above). Moreover, should personal data be transferred to a country located outside of the EEA, the controller must make sure that any of the exceptions to the general prohibition on transferring personal data to a third country applies or that another acceptable measure for the transfer has been taken (see Section 11 above). The controller may be obliged to provide the data subjects with information about the transfer of their personal data.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

Requirements to the handling of data security breaches are found in the Personal Data Regulation § 2-6. The requirements only apply to certain types of personal data of particular importance, namely such personal data for which it is necessary to “protect the confidentiality, availability and integrity” in order to “prevent the danger of loss of life and health, financial loss or loss of esteem and personal integrity”, and which are processed entirely or partly by “automatic means” cf. § 2-1. In case of a breach related to such data, measures must be taken to “re-establish the normal state of affairs, eliminate the cause of the discrepancy and prevent its recurrence”. Further, the Data Inspectorate must be notified if the breach “has resulted in the unauthorised
disclosure of personal data where confidentiality is necessary”. Finally, the results of handling of the security breach incident shall be documented. The Personal Data Act does not expressly require that the data subjects be notified of the breach, but doing so may still be required for other reasons, in particular if necessary in order to assist the data subject in avoiding a loss.

16. Accountability
Organizations implementing new information systems and/or technologies for the processing of personal data must first consider if the general conditions for such data processing are met. This means, among others, defining the purpose of the processing, considering if there is a legal basis to justify it, and integrating it in its security and internal control systems for personal data. This also means assessing the risks associated with the processing of personal data. Documentation of these assessments and systems must be made available upon request from the Data Inspectorate.

17. Whistle-blower hotline
Whistle-blower hotlines may be established in Norway, provided that general data privacy law requirements are observed. There is no obligation to establish whistle-blower hotlines, but doing so may be a way of meeting the requirements in the Working Environment Act to implement measures that facilitate the reporting of illegal activities in the business.

18. E-discovery
An employer’s right to access employee emails or other electronic information held by employees (even if work related and stored on the employer’s equipment) is subject to various restrictions. Firstly, the accessing must be justified by certain legitimate reasons as further defined, and secondly, certain procedures must be followed, which normally involve notifying the employee in advance and allowing the employee to be present. The rights of the employees are mandatory, and cannot be waived in advance.

19. Anti-Spam Filtering
Generally, the introduction of a spam filtering solution in an organization does not raise privacy issues. However, the individual control of such a spam filtering system will raise privacy issues (see Section 18 above).

20. Cookies
The Electronic Communication Act restricts the deployment of cookies. The consent of the user must be obtained before cookies can be used, with certain limited exceptions related partly to transfers of communication in electronic communication networks, and partly to information society services requested by the user. In practice, consent in the form of browser settings has been accepted. The use of cookies must in any case comply with general data privacy law requirements.
21. Direct Marketing

The Marketing Act restricts the use of direct marketing. Individual electronic communications for marketing purposes (such as email and SMS) to physical persons (whether in a business or consumer capacity) require either the prior consent of the recipient, or alternatively an already existing customer relationship with the recipient. Phone calls and non-electronic letters for marketing purposes cannot be sent to individuals listed in the Reservation Register.
Paraguay

Nestor Loizaga
Asuncion
Tel: 595 21 318 3000 ext. 117
nloizaga@ferrere.com
1. Recent Privacy Developments

There have been no major privacy developments in Paraguay.

The Paraguayan Constitution protects the right to privacy; it ensures the right to information and regulates the constitutional right known as habeas data as an instrument for data protection. *Habeas data* guarantees individuals the right to access information or data about themselves on official or private public record. It gives individuals the right to know how the information is being used and for what purpose, and allows for the updating, rectification or destruction if it was incorrect or illegitimate.

The first data protection legislation in Paraguay was enacted in the year 2001. Data protection and personal information are regulated and governed by Law No 1682/01 and its amendment Law 1969/02 (the “Law”). The Law regulates the collection, storage, distribution, publication, modification, destruction, duration and in general the treatment of personal data contained in files, registries, and databases and in general any other technical means of treatment of public or private data destined to provide reports, in order to ensure protection of Privacy in individuals.

The major challenge imposed by the Law is that it does not provide for a specific data protection authority. Consequently, when faced with infringements, individuals or legal entities are required to file individual complaints before ordinary civil courts. Although the Law aims at protecting personal data and information, the underlying issue is that this legal framework primarily addresses the protection of financial and credit information.

2. Emerging Privacy Issues and Trends

There have been no noteworthy emerging privacy issues in Paraguay.

3. Law Applicable

The legal framework for Data Protection in Paraguay comprehends the following:

- Paraguayan Constitution (Articles 4, 33, 34, 36 & 135).
- Law No. 1682/01 That Regulates Private Information.
- Law No. 1969/02 which amends and replaces several articles of Law No. 1682/01.
- Law No. 1160/97 “Paraguayan Criminal Code” and its amendments under Law No. 3440/08 and Law No. 4439/11.
4. Key Privacy Concepts

a. Personal Data
The Law does not contain a specific definition for “Personal Data”.

b. Data Processing
The Law does not contain a specific definition for “Data Processing”.

c. Processing by Data Controllers
The Law does not contain a specific definition for “Data Controllers”. Furthermore, no distinction is made between entities that hold or control personal information and data and those that process it on behalf of other entities.

d. Jurisdiction/Territoriality
The Law applies to any physical person or legal entity having a legal domicile or local offices or branches in Paraguay.

However, the Law does contain exemptions as it does not apply to databases or sources of journalistic information. It is also unenforceable against the freedom of expression and freedom to report or inform.

e. Sensitive Personal Data
The Law defines “sensitive data” as that which makes reference to racial or ethnic preferences, political preferences, individual health status, religious, philosophical or moral convictions, and sexual intimacy and in general anything that can promote prejudice and discrimination or that affects the dignity, privacy, or that may affect the domestic intimacy and private image of individuals or families.

f. Employee Personal Data
The Law does not contain a specific definition for “Employee Personal Data”.

5. Consent

a. General
There is no express requirement for an individual or legal entity to obtain consent when collecting, storing or processing personal data strictly for private use.

It is legal to collect, store, process and publish personal data for scientific and statistical purposes, for polls and public surveys as well as market research, provided that the publications do not individualize the person or legal entity investigated.

The only mandatory requirement for written consent refers to the publication of financial and credit information. The Law establishes that data and information that describe, reveal or estimate a patrimonial situation, economic
solvency or compliance of commercial and financial obligations, may only be published when individuals or legal entities have provided express written authorization for the collection of financial information concerning obligations that have not been claimed in a court of law.

b. **Sensitive Data**
The Law prohibits the publication and disclosure of sensitive data with regard to individuals who are explicitly individualized or identifiable.

However, the Law does authorize the publication of data solely consisting of the following: name and surname, identity card, address, age, date and place of birth, marital status, occupation or profession, work place and number.

c. **Minors**
There are no provisions that specifically address consent requirements for minors.

d. **Employee Consent**
There are no provisions that specifically address consent requirements for employees.

e. **Online/Electronic Consent**
There are no provisions that specifically address online or electronic consent, its admissibility and effectiveness. (Nonetheless, the validity of electronic and digital signatures are recognized under Paraguayan Law No. 4017/10.)

6. **Information/Notice Requirements**
On account of constitutional provisions and the rights set forth by the Law, entities that collect personal data must provide access to the data, as well as information regarding its use and the purpose for which the data was collected.

7. **Processing Rules**
There is no specific legislation on this matter or rules addressing this issue.

8. **Rights of Individuals**
The Law establishes that all individuals have the right to collect, store and process personal data exclusively for private use.

Furthermore, it sets forth that public sources of information are accessible to everyone. It establishes that individuals are entitled to access data and information regarding their property, themselves, their spouse and people under their guardianship or conservatorship contained in official or private registries of a public nature or in entities that provide information on financial solvency.
Individuals are entitled to know the use and the purpose for which the data and information was collected and request the correction of the personal data that is erroneous, inaccurate, misleading or incomplete.

9. Registration/Notification Requirements
There are no registration or notification requirements in Paraguay.

10. Data Protection Officers
Since no data protection authority was created under the Law, there is no requirement to appoint or designate data privacy officers who would be accountable for privacy practices.

11. International Data Transfers
There are no specific rules in Paraguay regarding international transfers of Personal Data. The Law does not establish any imposed restrictions to the cross-border transfer of personal information, nor the export of personal data to other jurisdictions.

12. Security Requirements
In general terms and except for certain regulated areas such as banking or tax, there is no specific requirement regarding security measures for the protection of Personal Data.

13. Special Rules for the Outsourcing of Data Processing to Third Parties
There is no specific legislation on this matter or rules addressing this issue.

14. Enforcement and Sanctions
As previously mentioned, no data protection authority was created under the Law.

The Law only contemplates monetary penalties in the event of non compliance or infringements by individuals or legal entities which publish, distribute, supply or disclose information that describes, reveals or estimates a patrimonial situation, economic solvency or compliance of commercial and financial obligations regarding individuals or legal entities. These penalties are also enforceable on individuals or legal entities which are obliged to rectify or provide the necessary information in order to rectify the aforementioned financial and economic solvency information and fail to do so within the legal term.

The fine shall be established according to the circumstances of each particular case and the amount varies from 50 to 200 minimum wages for diverse unspecified labor activities and can be doubled, tripled and so on in the event of recidivism.
Additionally, the affected party could file civil and criminal complaints before ordinary courts.

The Paraguayan Criminal Code provides that the infringement of communication and image are sanctioned with fines or imprisonment of up to two years.

The violation of confidentiality or the secrecy of communication is sanctioned with fines or imprisonment of up to one year.

The violation of security systems and unauthorized access to data is sanctioned with fines or imprisonment of up to three years. Unauthorized interception and transfer of data is sanctioned with fines or imprisonment of up to two years.

The violation of a person’s intimacy and the exposure of their intimacy are sanctioned with fines.

The disclosure of private secrets is punishable with imprisonment up to one year or fines. If the disclosure was made by a person obligated to maintain its secrecy due to their profession, the imprisonment shall be up to three years or a fine. The Disclosure of private secrets for economic purposes increases imprisonment to up to five years.

15. Data Security Breach

No specific legislation regulates the requirement of notice in the event of personal data compromise or privacy breach.

16. Accountability

There are no specific rules addressing this issue.

17. Whistle-Blower Hotline

There are is no specific legislation on this matter or rules addressing this issue.

18. E-Discovery

There are is no specific legislation on this matter or rules addressing this issue.

19. Anti-Spam Filtering

There is no specific legislation on this matter or rules addressing this issue.

However Article 23 of the Electronic Commerce Law No 4868/2013 regulates non-requested commercial communications sent via e-mail.
It determines that providers of goods and services can only send such communication when they comply with the following requirements:

a) Expressly indicate that it is a non-requested commercial communication;

b) Include an easy receipt exclusion system in the message;

c) The recipients data was not obtained through the infringement of his privacy rights; and

d) The communication does not exceed the size set forth by the authority.

20. Cookies

There are is no specific legislation on this matter or rules addressing this issue.

21. Direct Marketing

There is no specific legislation on this matter or rules addressing this issue. However Article 22 of the Electronic Commerce Law No 4868/2013 grants protection to user’s privacy by stipulating that providers of goods and services through electronic means, shall offer users or consumers the possibility to oppose the use of their data for promotional purposes by means of a simple and free procedure, at the time the data is collected and in every commercial communication sent to the user or consumer.
Peru

Viviana Chavez
Lima
Tel: +51 1 618 8500 Ext. 421
viviana.chavez@bakermckenzie.com

Javier Tovar
Lima
Tel: +51 1 618 8500 Ext. 550
javier.tovar@bakermckenzie.com

Teresa Tovar
Lima
Tel: +51 1 618 8500 Ext. 552
teresa.tovar@bakermckenzie.com
1. Recent Privacy Developments

The Data Protection Authority initiates the enforcement of Data Protection Law

In October 2014, the Authority imposed the first sanctions for non-compliance of Data Protection Legislation.

Two public officials filed two separate complaints against the website ‘datosperu.org’, because the company did not respond to their requests to eliminate from its webpage two resolutions (copied from the Official Gazette), through which one of them was removed from his office and the other one was disciplinarily sanctioned. The Resolutions were annulled by two subsequent resolutions; however such information was not published through datosperu.org webpage. The public officials alleged that datosperu.org did not let them exercise their cancellation right.

The Data Protection Authority sanctioned ‘datosperu.org’ with a fine equivalent to US$ 76,000.00 for violating the principles of consent and quality, and for not allowing public officials to exercise their ARCO rights:

- Regarding the principle of consent, the Authority sanctioned ‘datosperu.org’ since they did not anonymize the information of the Resolutions when including them in their database. Even though an exception for obtaining the consent is when the information is contained in “public available sources”, the Authority considered that the Official Gazette is not a regular public available source, but a repertoire of jurisprudence, which needs to be anonymized in order to be disclosed without the need of obtaining the consent. Since ‘datosperu.org’ didn’t anonymize the information, the Authority considered that it violated the principle of consent.

- Regarding the principle of quality, the Authority considered that as long as ‘datosperu.org’ did not include the subsequent resolutions - through which the sanctions to the public officials were annulled - the information published was inaccurate and, thus, the website violated the principle of quality.

- Finally, regarding the exercise of ARCO rights, the Authority sanctioned the company because the e-mail address published on the website for such purpose was not active.

To date, it has not been possible to collect the fine since the Authority has not yet determined who owns the web domain or identified the person who should be sanctioned.
2. Emerging Privacy Issues and Trends

The Data Protection Authority has the authority to issue opinions regarding the interpretation of the Data Protection Law - as requested by any individual or entity. Below are a few of the latest opinions enacted by the Authority:

- **Use of personal data published in social networks** - the Authority analysed if social networks could be considered as “public available sources”, concluding that they are not. As a consequence, the Authority considered that all information that users publish in their profiles is private and can not be used by another person without authorization. Bear in mind that this criterion applies to public and privates profiles, regardless how the user has set its profile using the website’s privacy tools.

- **Use of personal data for marketing purposes** - the Authority stated that personal data could be used by companies for a first contact, in order to request consent to send information about their products or services, as long as the contact is made on working days and at reasonable hours, is not performed in a persistent manner and the refusal of consumers to receive such information is respected. If the contact is made by e-mail, it must comply with the provisions of Anti-Spam Law. Contact can not be made if the data to be used to make the contact is registered in the “Do not call Registry” (Registro gracias… no insista) managed by the Consumer Protection Authority.

3. Law Applicable

The Peruvian Political Constitution recognizes the right to privacy as a fundamental right and provides for “habeas data”, a mechanism to protect such right - through a judicial process - in cases of commission of any act or omission that violates or threatens the expectation of privacy.

Nevertheless, the Peruvian data protection legal framework –Law N° 29733 and its Regulation approved by Supreme Decree N° 003-2013-JUS– seek to guarantee the fundamental right of privacy while recognizing specific rights of the Data Subject and obligations of those who are responsible for the processing of such data.

4. Scope of the Law

a. **Personal Data**

“Personal Data” is defined as any information regarding a natural person (“Data Subject”) that identifies it or makes it identifiable through means that can be reasonably used.
b. Data Processing

“Data processing” is defined as any operation or technical proceeding, automated or not, that allows the collection, storage, organization, modification, usage, suppression, transfer - among other actions – that allows the access, correlation or interconnection of Personal Data.

c. Processing by Data Controllers

The Law applies to the holders of the data bank (“Data Controllers”), who are the natural persons, private legal persons or public entities that process the Personal Data within a data bank and that must adopt the security measures to guard the Personal Data.

d. Jurisdiction/Territoriality

The Law applies to Personal Data contained or intended to be included in private or public databases whose processing is performed within the Peruvian territory. It is not applicable to Personal Data contained or intended to be included in databases created by natural persons for its private or family use, nor applicable to Personal Data contained or intended to be included in databases of public entities for the strict fulfillment of their responsibilities regarding national defense, public security and criminal investigation and repression.

e. Sensitive Personal Data

According to the Law, “Sensitive data” includes biometric data, data related to racial and ethnic origin; income; opinions or convictions regarding politics, religion, philosophy or morality; union membership; and information related to health or sexual life. The Regulations have stated that “Sensitive Data” is also the information referred to the emotional characteristics of a person; the facts and circumstances of its personal and familiar life; its personal habits; and information that corresponds to their most intimate sphere.

f. Employee Personal Data

There are no specific requirements on this regard, therefore, it is understood that the general provisions contained in the Law are applicable.

5. Consent

a. General

The processing of Personal Data requires prior, informed, express and unequivocal consent. Consent can never be implied.

The Law also states that consent will not be required in specific cases, among which are the following: (i) when it relates to a person’s health: (a). when necessary in a situation of risk, prevention, diagnosis or medical or surgical treatment of the owner of the information, if such processing is carried out by a medical institution or by health professionals, complying with the professional secret; (b). for public health reasons, or; (c). for the realization of
epidemiologic or analogous studies; (i) when the Personal Data is public information, (ii) when it is related to the financial solvency or creditworthiness of a person; (iii) when necessary for the execution of a contractual relationship; (iv) others to be established in regulations of the Data Protection Law and those established in other laws.

b. Sensitive Data
When referring to Sensitive Data, the prior, informed, express and unequivocal consent must be granted in writing.

c. Minors
Consent can be obtained from minors as long as they are 15 or above, provided that the information given to them at the time of collection is expressed in a comprehensive language and the products or services offered are not restricted to their age. Regarding minors below 15 years, the consent must be obtained from their legal representatives.

d. Employee Consent
There are no specific requirements on this regard, therefore, it is understood that the general provisions contained in the Law are applicable.

e. Online/Electronic Consent
Electronic consent is permissible and can be effective in Peru if properly structured and evidenced.

6. Information/Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Subject; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to exercise the rights recognized by the legal framework; and the term during which the information will be stored.

7. Processing Rules
An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications;
request the correction of the Data Subject's Personal Data; request the deletion and/or destruction of the Data Subject's Personal Data; impede its transference to third parties and exercise the writ of habeas data.

In exercising the right to access Personal Data (when it comes to data bases of public administration), the Data Subject may have to shoulder the costs for producing the same (e.g., costs for photocopying the documents).

9. Registration/Notification Requirements

The Law creates the National Registry for the Protection of Personal Data ("Registry"), which is open to the public. The Registry is in charge of the National Authority for the Protection of Personal Data, for the purposes of registering:

- The private or public databases and the information about Data Subjects that would be necessary for the exercise of their rights.
- The authorizations issued under the Regulations.
- The sanctions, precautionary and corrective measures imposed by the National Authority for the Protection of Personal Data.
- The codes of conduct of the entities that manage private databases.

Communications regarding cross-border transfers of data.

10. Data Protection Officers

Organizations may be required to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

International transfer of Personal Data requires consent from the owner of the information and can be made only if the recipient country has adequate levels of protection, similar to those under the Law.

If the recipient country does not have an adequate level of protection, the data transmitter must guarantee that the processing of the Personal Data will be made according to the Law. This is not applicable if:

(i) the transmission of Personal Data conducted within the framework of an international judicial cooperation or the application of international trades on this regard;
(ii) international cooperation among intelligence agencies;
(iii) when the Personal Data are necessary for the execution of a contractual relationship in which the Data Subject is part of;
(iv) when referring to banking and security transfers.
(v) when the transfer is made for the purposes of protecting, preventing, diagnosing and for providing medical treatment to the Data Subject
(vi) when the Data Subject has granted his/her consent for the transfer of data under these conditions.
(vii) when the Personal Data is necessary for the development of a scientific or professional relationship in which the Data Subject is part of.

In case of cross-border transfer of Personal Data, organizations are required to notify the data authority.

12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
If the Data Controller outsources the processing of the Personal Data to a third party (“the Processor”), such party must also comply with the Law (keeping the confidentiality of the information processed; using the Personal Data only for the purposes authorized; modifying inaccurate information, among others).

After the execution of the outsourcing agreement, the Personal Data processed must be removed, unless Data Subject provides express consent to do otherwise.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits/ data authority orders, administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
There are no specific rules addressing data security breaches. However, as Data Controllers are generally liable for any data security breach, it is highly advisable to inform the affected Data Subjects as soon as the Data Controller becomes aware of a data security breach.

Organizations that are involved in a data breach situation are required to take steps to mitigate the harm to impacted Data Subjects; take steps to contain the breach; take steps to prevent future similar breaches; assist authorities
with any investigation relating to the breach; and comply with data authority orders and court orders.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, civil actions and/or class actions, or a criminal prosecution.

16. Accountability
Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
There are no specific legal references on this regard. Nevertheless, if the data obtained as a consequence of the implementation of a whistle-blower hotline is collected by the Data Controller for creating a data bank, such data bank should be registered before the National Authority for the Protection of Personal Data.

18. E-Discovery
There is no law/rule that regulates e-discovery in Peru.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace, and give employees the opportunity to opt-out from the spam-filtering solution.

20. Cookies
There are no specific laws/rules in Peru that regulate the use and deployment of cookies. In general, the use and deployment of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. Consent of the Data Subject must be obtained for a specific activity. Bundled consent is not considered valid consent. See also Section 2 (Use of personal data for marketing purposes)
Philippines

Carlo Abarquez
Manila
Tel: +63 2 819 4993
carlo.abarquez@quisumbingtorres.com

Bienvenido Marquez
Manila
Tel: +63 2 819 4936
bienvenido.marquez@quisumbingtorres.com

Divina Ilas-Panganiban
Manila
Tel: +63 2 819 4961
divina.ilas-panganiban@quisumbingtorres.com
1. Recent Privacy Developments

_Supreme Court of the Philippines decides that Filipinos have no right to informational privacy on Facebook_

In the recent case of _Vivares et al. v STC et al._¹, the Supreme Court of the Philippines ruled that the right to privacy over one’s personal information posted on _Facebook_ can be determined by the privacy settings chosen by the user. The highest level of expectation of privacy occurs when privacy settings are set to “only me”. One should have no expectation of privacy when the privacy settings are set to “public”. The court held that “utilization of these privacy tools is the manifestation, in cyber world, of the user’s invocation of his or her right to informational privacy”².

The case stemmed from complaints of parents against a school for preventing (on disciplinary grounds) their daughters from attending their high school graduation. The school, run by Catholic nuns, admonished the daughters of the complainants for posting on _Facebook_ photographs of them wearing only their undergarments, drinking alcoholic beverages and/or smoking. The school learned of the photographs after several other students of the school (who were friends of the girls on _Facebook_) provided them with the photos.

The court ruled that the daughters indeed had expectations of privacy, but since their privacy settings on _Facebook_ were set to “public” or “friends”, their expectation of privacy is limited. Thus, the manner in which the school acquired the photos was not illegal or in contravention of the girls’ right to privacy. The court added that the complainants and their daughters have a cause of action against those students who provided the photos to the school, but not against the school itself. The court then provided a discussion on cyber responsibility, discussing, among others, that “self-regulation on the part of Online Social Network users and Internet consumers in general is the best means of avoiding privacy rights violations”.

2. Emerging Privacy Issues and Trends

There are no emerging privacy issues in the Philippines.

3. Law Applicable

Republic Act No. 10173 or the Data Privacy Act of 2012 is the main legislation governing data privacy in the Philippines.

Prior to the Act, there was no Philippine law dealing specifically with data privacy. While the Philippine Constitution and jurisprudence recognize and protect a person’s right to privacy, it deals with protection of personal information in a general manner.

---

¹ G.R. No. 202666, 29 September 2014
² Informational privacy refers to the right of individuals to control information about themselves.
There are also provisions scattered across several statutes, such as the Civil Code, the Revised Penal Code, the Anti-Wire Tapping Law, and the Electronic Commerce Act, dealing with the right of privacy of an individual. However, these provisions do not squarely address the issue of data privacy and so were inadequate and, in some instances, inapplicable, in addressing the issue of Personal Data privacy. There is also no government agency overseeing the protection of Personal Data.

4. Key Privacy Concepts

a. Personal Data

The Act defines “Personal Information“ as any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

b. Data Processing

The Act defines “Processing“ as any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

c. Processing by Data Controllers

Under the Act, a personal data controller may transfer personal information to a third party for processing. However, the personal data controller remains responsible for such data and remains accountable for compliance with the Act.

d. Jurisdiction/Territoriality

The Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:

(a) The act, practice or processing relates to personal information about a Philippine citizen or a resident;

(b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:

(1) A contract is entered in the Philippines;

(2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and

(3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and
The entity has other links in the Philippines such as, but not limited to:

1. The entity carries on business in the Philippines; and
2. The personal information was collected or held by an entity in the Philippines.

However, personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, are not covered by the provisions of the Act even if the personal information is being processed in the Philippines.

e. Sensitive Personal Data

Under the Act, “sensitive personal information” refers to personal information:

1. About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. About an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an executive order or an act of Congress to be kept classified.

f. Employee Personal Data

Under the Act, there is no substantial difference between the rules applicable to employee data and any other kind of personal data.

Employees are not entitled to be notified when the following information entered, collected and processed in the processing system of the employer are for obvious purposes:

1. Description of the personal information to be entered into the system;
2. Purposes for which they are being or are to be processed;
3. Scope and method of the personal information processing;
4. The recipients or classes of recipients to whom they are or may be disclosed;
5. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
(6) The identity and contact details of the personal information controller or its representative;

(7) The period for which the information will be stored; and

(8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the National Privacy Commission.

5. Consent Requirements

a. General

The Data Privacy Act differentiates “personal information” from “sensitive personal information” and provides for their different treatment. The processing of personal information is permitted, if not otherwise prohibited by law and when at least one of the conditions stated in the law exists. On the other hand, the processing of sensitive personal information is prohibited, except in specific instances enumerated under the law. For both types of information, however, consent of the data subject is the common underlying requirement for processing to be considered lawful. To be valid, “consent” must be freely-given, specific, informed. The purpose for which the collection of information is done must be specific, legitimate and made known to the data subject before, or as soon as reasonably practicable after collection, and information must later be processed in way compatible with such declared, specified and legitimate purpose. For sensitive personal information, in particular, the consent must be specific to the purpose and obtained prior to the processing of such information.

b. Sensitive Data

See Section 4(e).

c. Minors

A minor cannot consent to the collection of his or her personal information. Consent must be obtained from the parents or legal guardian.

d. Employee Consent

There is no provision that specifically addresses consent requirements for employees. But the general rule on collection of personal information about individuals applies.

e. Online/Electronic Consent

Electronic consent is allowed. Under the Act, consent shall be evidenced by written, electronic or recorded means.

6. Information/Notice Requirements

The data subject is entitled to:

(a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;
(b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:

1. Description of the personal information to be entered into the system;
2. Purposes for which they are being or are to be processed;
3. Scope and method of the personal information processing;
4. The recipients or classes of recipients to whom they are or may be disclosed;
5. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
6. The identity and contact details of the personal information controller or its representative;
7. The period for which the information will be stored; and
8. The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the National Privacy Commission.

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification to the data subject. However, the notification under subsection (b) shall not apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of a legal obligation.

7. Processing Rules

Processing of personal information must adhere to the principles of transparency, legitimate purpose and proportionality. The specific processing rules are expected to be detailed in the implementing rules and regulations for the Act.

8. Rights of Individuals

A Data Subject is entitled to reasonable access to, upon demand, the following:

1. Contents of his or her personal information that were processed;
2. Sources from which personal information were obtained;
3. Names and addresses of recipients of the personal information;
4. Manner by which such data were processed;
(5) Reasons for the disclosure of the personal information to recipients;

(6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

(7) Date when his or her personal information concerning the data subject were last accessed and modified; and

(8) The designation, or name or identity and address of the personal information controller;

In addition to the foregoing access rights, generally, a Data Subject is entitled to:

(a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;

(b) Subject to certain exceptions, be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:

1. Description of the personal information to be entered into the system;

2. Purposes for which they are being or are to be processed;

3. Scope and method of the personal information processing;

4. The recipients or classes of recipients to whom they are or may be disclosed;

5. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;

6. The identity and contact details of the personal information controller or its representative;

7. The period for which the information will be stored; and

8. The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of Data Subject.

(c) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the
personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof:

Provided, That the third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon reasonable request of the data subject;

(d) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller’s filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information;

(e) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information; and

(f) Where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject.

9. Registration/Notification Requirements

At present, no specific registration requirements apply.

The personal information controller shall promptly notify the National Privacy Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

(1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with Section 20 of the Act (Security of Personal Information) and existence of good faith in the acquisition of personal information.
(2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.

(3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Kindly note that, upon this submission, the Commission has not yet been organized.

10. Data Protection Officers

There is no requirement under the Act for appointment of a data protection officer. The Act, however, requires a personal information controller to designate an individual or individuals who are accountable for the organization’s compliance with the Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

11. International Data Transfers

The Data Privacy Act does not appear to specifically require that personal information collected from Philippine citizens or residents should be stored or processed in the Philippines. It also does not appear that the Act prohibits the off-shore storage or the transfer of such personal information to foreign jurisdictions. The Act, however, considers the “personal information controller” to continue to be responsible for personal information that may have been “transferred to a third party for processing, whether domestically or internationally.”

There is an old law, Presidential Decree 1718, that prohibits the transfer of documents or information relating in any manner to any business carried on in the Philippines, unless such taking, sending or removal is:

- consistent with and forms part of a regular practice of furnishing to a head office or parent company or organization outside of the Philippines;
- in connection with a proposed business transaction requiring the furnishing of the document or information;
- required or necessary for negotiations or conclusions of business transactions, or is in compliance with an international agreement to which the Philippines is a party; or
- made pursuant to the authority granted by the designated representative(s) of the President.

The Office of the President has yet to issue rules and regulations implementing the law since its passage on August 21, 1980. Hence, the law is not strictly enforced.
12. Security Requirements

The Act requires that:

(a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

(b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

(c) The determination of the appropriate level of security must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:

(1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;

(2) A security policy with respect to the processing of personal information;

(3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and

(4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

(d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

(e) The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.
13. Special Rules for the Outsourcing of Data Processing to Third Parties

Under the Act, a personal information controller may subcontract the processing of personal information. However, the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the Act and other laws for processing of personal information. The personal information controller remains responsible for the personal information, even information that has been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. The Act further makes the personal information controller accountable for complying with the requirements of this Act and requires him/her to use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.

14. Enforcement and Sanctions

Potential civil, administrative, or criminal sanctions may be imposed for specific violations of the Act (e.g., unauthorized processing, accessing due to negligence, improper disposal, processing for unauthorized purposes, unauthorized access or intentional breach, concealment of security breaches, malicious disclosure, and unauthorized disclosure of personal information and sensitive personal information.)

15. Data Security Breach

The personal information controller shall promptly notify the National Privacy Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

(1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with Section 20 of the Act (Security of Personal Information) and existence of good faith in the acquisition of personal information.
(2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.

(3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Kindly note that, upon this submission, the Commission has not yet been organized.

16. Accountability

There is no law in the Philippines that requires an organization to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-blower hotline

There are no laws/rules that govern whistle-blower hotlines in the Philippines.

18. E-discovery system

The Data Processor is required to obtain the consent of the members or employees prior to the implementation of an e-discovery system which monitors and stores electronic information.

19. Anti-spam Filtering

A spam-filtering solution may arguably be considered a violation of the right to privacy of communications of the persons within the organization. To eliminate or minimize the risk of privacy violation issues, the consent of the individuals/employees should be obtained.

20. Cookies

There are no laws/rules that govern the use and deployment of cookies in the Philippines.

21. Direct Marketing

There are no laws/rules that regulate direct marketing in the Philippines.
Poland

Jakub Falkowski  
Warsaw  
Tel: +48 22 445 3294  
jakub.falkowski@bakermckenzie.com

Magdalena Kogut-Czarkowska  
Warsaw  
Tel: +48 22 445 3452  
magdalena.kogut-czarkowska@bakermckenzie.com

Radosław Nożykowski  
Warsaw  
Tel: +48 22 445 3210  
radoslaw.nozykowski@bakermckenzie.com
1. Recent Privacy Developments

Facilitation of the Exercising of Economic Activity Act

The Facilitation of the Exercising of Economic Activity Act entered into force on 1st January of 2015. The new statute introduced some important changes to the Act on the Protection of Personal Data (“PPD”). In particular:

1. provided new means to legitimize Personal Data transfers to countries outside of the EEA that do not offer adequate levels of protection. Now, such transfers are also allowed if the parties execute a data transfer agreement based on an unmodified version of the European Commission’s Standard Model Clauses, or implement binding corporate rules approved by the Inspector General for Personal Data Protection (GIODO);

2. changed the legal position and responsibilities of the Data Protection Officer. New tasks of the Data Protection Officer include keeping an open register of data filing systems processed by the company and conducting internal investigations, at the request of GIODO, to verify that the processing of personal data by the company is compliant with the provisions of the PPD;

3. limited notification requirements of data filing systems. Companies which appoint a Data Protection Officer and notify GIODO about the Data Protection Officer are released from the obligation to register the electronic data filing systems, unless sensitive data are processed.

For global companies the most important change seems to be that it is a liberalization of the rules regarding the transfer of Personal Data outside the EEA.

New DPA in Poland

On 3 December 2014 the Polish parliament accepted the resignation of the GIODO, Mr. Wiewiórowski. He resigned due to his being chosen as the Assistant European Data Protection Supervisor in Brussels. In April 2015, Dr. Edyta Bielak-Jomaa was appointed and sworn in the office to serve as the next GIODO. Dr. Bielak-Jomaa is a lawyer and an academic specializing in privacy and labor law.

Direct marketing

The brand new Consumer Rights Act of 30 May 2014, which entered into force on 25 December 2014, amended the rules of direct marketing in the telecommunication law. It strictly forbids the use of telecommunications terminal equipment or automated calling systems for direct marketing purposes, unless the subscriber or end user has previously given his/her consent. This prohibition applies to both spam and unsolicited phone calls.
The protection is granted to all natural or legal persons, regardless of their status as a consumer.

2. Emerging Privacy Issues and Trends

Medical records

The Ministry of Health is working on an amendment of the Patient’s Rights Act of 8 November 2008. According to the proposed bill, the right to access a patient’s medical records would be granted also to emergency medical technicians, students of medicine, the hospital’s secretary or archivist. Additionally, the information reported to an emergency’s dispatcher is to be excluded from the definition of medical records.

Other proposed changes concern the manner of access to medical records by patients (the project clarifies that the patient is to receive only a copy of the records and not the originals) as well as the rules for handling the medical records in case of the physician’s death or the hospital’s liquidation.

New economic law

The project on the new economic law, which is being developed by the Ministry of Economy, proposes to remove from the definition of Personal Data any information on the entrepreneur that has been disclosed in the publicly available Central Register of Information on Business (CEIDG). A similar provision already existed once in Polish law, but was repealed a few years ago. This change may have significant implications for companies collecting and processing business contact data.

3. Law Applicable

The processing of Personal Data in Poland is regulated by the Law on the Protection of Personal Data (“PPD”) of August 29, 1997 (as amended), and the Ordinance of the Minister of Internal Affairs and Administration of 29 April 2004 specifying the documentation of processing Personal Data and the technical and organizational requirements which should be fulfilled by equipment and computer systems used for processing Personal Data (“Ordinance”). Furthermore, the Minister of Administration is working on an ordinance specifying the tasks of the Data Protection Officer, which should enter into force later this year. In general, the PPD implements the provisions of EU Data Protection Directive (95/46/EC).

The PPD applies to the processing of Personal Data in files, indexes, books, lists and other registers, as well as those contained in computer systems (even if they do not constitute a data filing system).

With regard to the collection of Personal Data which are compiled on a short term basis exclusively for technical or training purposes or in connection with teaching purposes in schools of higher education, and which, upon being used are immediately removed or treated so as to make them anonymous,
only limited provisions of the PPD apply, in particular those related to security requirements.

Apart from the PPD, several other statutes provide specific provisions regarding personal data protection, e.g. the Act on Providing Services through Electronic Means. Also, Article 173 of the Telecommunication Law refers to the use of cookies.

Links:

4. Key Privacy Concepts

a. Personal Data
The PPD applies to the processing of any information (“Personal Data”) relating to an identified or identifiable natural person (“Data Subject”).

b. Data Processing
“Processing” is broadly defined to include collection, recording, storage, organizing, changing, disclosure, and deletion. The PPD regulates both automated and manual data processing.

c. Processing by Data Controllers
The PPD applies to those natural persons, legal entities or organizational units who determine the purposes for which and the manner in which any Personal Data is, or is to be, processed (“Data Controllers”). Certain provisions of the PPD apply also to persons to which the Data Controllers entrust the processing of Personal Data (“Data Processors”).

d. Jurisdiction/Territoriality
The PPD applies in particular to data processing activities carried out by:

- Data Controllers that have their registered seat or place of residence in Poland; and
- Data Controllers that have their registered seat or place of residence in a third country, i.e., a country outside the EEA, but use technical means based in Poland to carry out data processing activities (other than merely for the purpose of transit).

e. Sensitive Personal Data
The PPD imposes additional requirements for the processing of sensitive Personal Data – that is, information revealing racial or ethnic origin, political opinions, philosophical or religious beliefs, religion, party or trade-union membership, health, genetic code, sexual life, convictions, penal judgments, fines, and other decisions issued in court or administrative proceedings.
Specifically, the processing of sensitive Personal Data is prohibited, unless certain conditions are met, including:

- the Data Controller obtains the written consent of the Data Subject (see Section 5(b) below), unless the processing consists of deletion of Personal Data;
- the provisions of other specific statutes provide for the processing of such Personal Data without the need to request the Data Subject’s consent and provide adequate safeguards;
- processing is necessary to protect the vital interests of the Data Subject or of other persons where the Data Subject is physically or legally incapable of giving his consent until a guardian or a curator is appointed;
- processing is necessary for the purpose of carrying out the statutory objectives of churches and other religious unions, associations, foundations, and other non-profit-seeking organizations or institutions with a political, scientific, religious, philosophical, or trade union aim and on the condition that the processing relates solely to the members of those organizations or institutions, or to persons who have regular contact with them in connection with their activities, and subject to providing suitable protection of the processed Personal Data;
- processing relates to Personal Data necessary for the establishment of legal claims;
- processing is necessary for the purpose of carrying out the obligations of the Data Controller with regard to employment of its employees and other persons, and the scope of processing is provided for by the law;
- processing is required for the purpose of preventative medicine, the provision of care or treatment, where the Personal Data is processed by a health professional involved in treatment, other health care services, or the management of health care services and subject to providing suitable protection for the Personal Data;
- processing relates to Personal Data that is manifestly made public by the Data Subject;
- processing is necessary to conduct scientific research, including preparation of a thesis required for graduating with or receiving a university degree; any results of scientific research cannot be published in a way which allows Data Subjects to be identified; or
- processing is conducted by a party in court or administrative proceedings in order to exercise rights and duties resulting from decisions issued in those proceedings.
f. Employee Personal Data

Employee Personal Data is likely to include non-sensitive and sensitive Personal Data (e.g., trade union membership information). Sensitive employee Personal Data may be processed in the circumstances identified in Section 4(e) above. Under the Polish Labor Code, an employer has the right to demand from employees the following non-sensitive Personal Data:

- given name(s) and surname;
- parents’ given names;
- date of birth;
- address (and mailing address);
- details of education; and
- details of employment history.

Once the candidate is employed, the employer has the right to demand Personal Data other than the types of Personal Data listed above, including:

- names, surnames, and dates of birth of employees’ children, provided that such data is required for the employee to benefit from special rights as provided for in the labor law;
- the PESEL number of each employee;
- Personal Data other than that provided for above, if the obligation to provide such data arises under other provisions of law (i.e., other than the Polish Labor Code).

5. Consent

a. General

Under Polish Law, consent of the Data Subject is not mandatory, but it is contemplated as a justification for the processing of Personal Data (i.e., may constitute a basis for the processing in case another statutory basis does not apply). In practice, it is often one of the more straightforward ways to justify processing. Consent must be express and cannot be presumed or implied from any other consents or declarations. Consent must be voluntary, informed and unambiguous. Written consent is not required. The language of consent must not be too abstract – that is, consent must not refer to processing of Personal Data in general. Consent must refer to a particular situation and particular categories of Personal Data and should clarify the methods and the purposes of such processing. Consent may be unlimited in time or provide for a certain timeframe. Data Subjects may withdraw their consent for data processing at any time.
b. **Sensitive Data**

The PPD imposes additional requirements for the processing of sensitive Personal Data, which includes information relating to racial or ethnic origin, political opinions, philosophical or religious beliefs, religion, party or trade-union membership, health, genetic code, sexual life, convictions, penal judgments, fines, and other decisions issued in court or administrative proceedings. Sensitive data may, however, still be processed without obtaining the written consent of the Data Subject in certain prescribed circumstances.

c. **Minors**

A person under the age of 18 cannot give valid consent. A parent or legal guardian must give consent on such minor’s behalf.

d. **Employee Consent**

Under Polish Law, consent is not required from an employee for the processing of Personal Data because processing of employees’ Personal Data for employment purposes is derived from legal provisions. The rulings of the Supreme Administrative Court, however, provide that an employer cannot seek employee consent for the processing of Personal Data outside the statutory scope.

e. **Online/Electronic Consent:**

Polish law does not prescribe any particular form in which consent should be given (exceptions apply to Sensitive Data, which in general requires written consent). However, bearing in mind the general principle that consent must not be implied, and also that it is the Data Controller who has to prove that it processes Personal Data in a lawful manner, electronic consent may not be sufficient.

6. **Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity, the purposes for collecting Personal Data, third parties to which the organization will disclose the Personal Data, and the rights of the Data Subject.

7. **Processing Rules**

An organization that processes Personal Data must: limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; anonymize the data whenever possible; and delete/anonymize personal information once the stated purposes have been fulfilled and legal obligations met.
8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

Generally, the PPD imposes on a Data Controller a general obligation to register a Personal Data database with the GIODO; however, some exceptions apply. In particular, such exceptions apply if the Personal Data (other than Sensitive Data) is not processed with the use of computer systems or if the Data Controller appointed a Data Protection Officer and notified him/her to GIODO.

The Data Controller may commence processing of a database upon submitting the database to the GIODO for registration. However, the Data Controller may start the processing of Sensitive Data in the database only after registration of the database.

10. Data Protection Officers

a. General and conditions

In Poland, organizations may appoint a Data Protection Officer. The appointment is voluntary. The Data Protection Officer must fulfill the following conditions:

- have full legal capacity and full public rights;
- have no criminal record for intentional crimes;
- have sufficient knowledge of Personal Data protection.

The appointment and the recalling of the Data Protection Officer should be notified to GIODO.

b. Tasks

The tasks of the Data Protection Officer include:

- ensuring compliance with the provisions on processing Personal Data in the organization;
- preparing periodic and ad-hoc (special) reports for the Data Controller;
- supervising the preparation and update of documentation on Personal Data processing and compliance with the rules provided in this documentation;
ensuring that the persons authorized to process Personal Data are familiar with the data protection laws;

• keeping a publicly available register of the databases held by the Data Controller.

c. Legal Position

The Data Protection Officer must answer directly to the “head of organizational unit” or the natural person who acts as the Data Controller. The Data Controller must create the conditions and “separation within its organization” necessary for the independent exercise of tasks by the Data Protection Officer.

11. International Data Transfers

a. General

International data transfers to a country that does not provide in its territory an adequate level of data protection may take place subject to the prior consent of the GIODO, issued by way of an administrative decision, provided that the Data Controller ensures adequate safeguards with respect to the protection of the privacy, rights and freedoms of the Data Subject.

GIODO does not recognize US law generally as providing a level of protection equivalent to that of Poland. However, if a data importer in the US is a Safe Harbor registered company, the GIODO takes a view that the requirement of providing an equivalent level of protection is met.

b. Exceptions

There are certain exceptions to the general rule against transfer of Personal Data to territories with inadequate data protection laws, the most relevant being where:

• the transfer is required by other laws or by the provisions of any ratified international agreement, which guarantee adequate level of Personal Data protection;

• the Data Subject has given his written consent;

• the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or takes place in response to the Data Subject’s request;

• the transfer is necessary for the performance of a contract concluded in the interests of the Data Subject between the Data Controller and a third party;

• the transfer relates to Personal Data that has been made public;
the transfer is necessary on public interest grounds or for the establishment, exercise, or defense of legal claims; or

- the transfer is necessary to protect the vital interests of the Data Subject.

c. Data transfer agreements

Data transfer agreements can render Personal Data transfer legitimate. The GIODO’s approval is not required if the Data Controller ensures adequate safeguards for the protection of privacy and the rights and freedoms of the Data Subject by applying binding corporate rules approved by the GIODO or standard contractual clauses approved by the European Commission.

12. Security Requirements

Organizations are required to take steps to: ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect personal data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. They are also required to comply with sector specific requirements. Furthermore, organizations that outsource the processing of data shall be held liable together with the third party provider in case of breach by the latter.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

In general, there is no legal obligation under the PPD to provide notice of a data security breach. Exception applies to the providers of publicly available telecommunication services, which must inform GIODO about security breach no later than within 3 days. The Data Protection Officer usually keeps records of data security breaches, which identify and describe the breach and the measures taken to address the breach (e.g., remedies implemented to prevent future breaches). In case of an audit, such records should be produced to the GIODO. Furthermore, organizations that are involved in data breach situations are required to: gather information about the breach; assess the potential risk of harm to Data Subjects; take steps to mitigate the harm to impacted Data Subjects; take steps to contain the breach and to prevent
future similar breaches; and assist authorities with any investigation relating to the breach.

An organization that is involved in a data breach situation may be subject to closure or cancellation of the file, register or database, civil actions, and/or criminal prosecution.

16. Accountability

Organizations are required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-blower hotline

There are no specific provisions regarding whistle-blower hotlines. Thus, the processing of Personal Data collected via whistle-blower hotlines is subject to the general provisions of the PPD. To the extent that data collected via whistle-blower hotlines concern employees, the employer is not required to comply with the obligation to provide notice of the data processing to the GIODO. Finally considering that the GIODO usually follows the opinions of the Article 29 Working Party, the guidelines of document WP 117 should be observed.

18. E-discovery

Implementing an e-discovery process in which electronically-stored information is reviewed, processed and presented by an organization for the purposes of litigation or regulatory requests may raise questions as to (i) the legal basis of processing the data contained in the electronically-processed information, as well as, (ii) the right of privacy of the employees in the organization. For this reason employers should inform their employees of the implementation of an e-discovery system, including the monitoring of electronic communications. Nevertheless, employees may request the employer to destroy any private information stored as a consequence of the implementation of the e-discovery system.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.

20. Cookies

There are specific laws that regulate the deployment of cookies. The Telecommunications Law provides for specific rules regarding the use and collection of data by means of the deployment of cookies, in order to secure the privacy of end users. Additionally, the use of cookies must comply with data privacy laws.
Consent of data subjects must be obtained before cookies can be used.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. An organization must obtain consent for a specific activity. Bundled consent is not considered valid consent.

It is forbidden to use telecommunications terminal equipment or automated calling systems for direct marketing purposes, unless the subscriber or end user has previously given his/her consent. Use of the above-mentioned measures for the purpose of direct marketing cannot be done at the expense of the consumer.
Portugal

César Bessa Monteiro
Lisbon
Tel: 351 21 326 4747
c.monteiro@pbbr.pt

César Bessa Monteiro, Jr.
Lisbon
Tel: 351 21 326 4747
cesar.bmonteiro@pbbr.pt

Ricardo Henriques
Lisbon
Tel: 351 21 326 4747
ricardo.henriques@pbbr.pt
1. Recent Privacy Developments

Geolocation devices in an employment context

The Portuguese Data Protection Authority ("CNPD") approved on 28 October 2014 Guidelines 7680/2014, which establish the general principles regarding the processing of personal data as a result of the use of geolocation devices in an employment context.

These Guidelines intend to impose several obligations to companies and public entities, in order to guarantee the balance between business management and organization, and the employee’s constitutional right to privacy.

Geolocation devices are technological means which make it possible to know the geographical location of an object or a person. In an employment context, these devices are mainly used in vehicles, smartphones or laptops owned by the employer but made available to the employee to perform his professional activity.

The CNPD considers that the use of such geolocation devices represents processing of sensitive data stipulated in paragraph 2 of Article 20 of the Portuguese Labour Code. This provision allows the employer to use means of remote supervision in the workplace being, for this reason, legitimate grounds for processing data.

On the other hand, the CNPD considered that consent given by the employees does constitute valid grounds for processing this type of data.

According to the above-mentioned Guidelines, geolocation data must be adequate, relevant and not excessive in relation to the purposes for which it was collected and will be processed. Geolocation is expressly prohibited for the following purposes:

1. Employee performance control;
2. Proof of compliance of contractual obligations;
3. Ensuring compliance with road traffic legislation;
4. Tracking the vehicle when it is being used for private purposes.

As for vehicles, CNPD has admitted processing data resulting from the use of geolocation devices on a working environment, with the following purposes:

1. Fleet management on external service – (i) external technical assistance or home assistance, (ii) goods distribution, (iii) passenger transportation, (iv) goods transportation and (v) private security;
2. Goods Protection – (i) criminal investigation and goods recovery in case of theft, (ii) transportation of dangerous materials and (iii) high value materials.
Regarding smartphones and laptops, the CNPD stated that the employer cannot use geolocation devices on these equipments or access the information when available by telecommunications operators or install mobile applications on smartphones which activate GPS sensors. However, the CNPD has considered admissible the installation of MDM (Mobile Device Management) technologies to ensure the remote protection of companies’ information.

This Guideline also covers the situations of knowledge by the employer of criminal evidence resulting from the processing of sensitive data. In this case, the CNPD has declared that this information can be used, under certain circumstances, as grounds for criminal and disciplinary proceedings.

The Employer must inform the employees of the existence of geolocation devices especially when these equipments are incorporated in cars, smartphones or laptops used by them to perform their work.

Finally, controllers of sensitive data intending to implement geolocation technology must file an authorization with the CNPD by means of a specific form available in http://www.cnpd.pt/bin/legal/forms.htm for such processing of sensitive data.

*Monitoring of the use of information technologies for private purposes in the workplace*

The CNPD has also issued Guidelines 1638/2013 concerning the personal data processing for the monitoring of the use of information technologies for private purposes in the workplace.

In general terms, these Guidelines established that when an employer monitors the use of e-mail, calls and/or Internet usage to verify if the use by the employee is only for professional purposes or also for excessive private (non-permitted use), then it needs to have an adequate policy in place and obtain a prior authorization from the CNPD.

Employers should adopt security measures that do not include a specific verification of the employee’s private information, even if it is intended to use it for disciplinary purposes. Additionally, it is determined that employers should adopt specific security measures, namely: implement measures to avoid the access to the information by non-authorized personnel; use registration to identify the user; restrict access to servers; in order to monitor correctly the information is necessary to implement logs that register who made such access, date and hour (timestamp), to control the operations made through such access by a sequential number (id), and a hash field to the previous elements should be applied.
It is also stated that the controller should identify all irregular situations in order to develop an alarm system that allows the identification of its irregular use. A policy concerning the use of logs should be implemented, as well as periodic analysis reports should be prepared. Finally, it is determined that such logs can only be stored for a maximum period of one year.

2. Emerging Privacy Issues and Trends

Cookies

An emerging privacy issue concerns the adequacy of the implementation of Directive 2009/136/EC transposed by Law 46/2012, of August 29th, more particularly the issue as to how informed consent for the use of cookies or other tracking technologies must be obtained.

The above mentioned Law 46/2012, of August 29 determined that:

1. The storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user shall only be allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information about the purposes of the processing;

2. The data controller must give users the possibility to withdraw their consent freely and in an easy manner.

3. Nevertheless, the consent requirement does not prevent any technical storage or access of data:

   a) For the sole purpose of carrying out the transmission of a communication over an electronic communications network;

   b) As strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

Regarding cookies, there are no Guidelines issued by the CNPD that clarify how they should actually be implemented. Companies in the market have taken different approaches on the implementation of this law requirement of obtaining consent for the use of cookies. Most use a banner on the front page of the website. However, whilst there are some that opt for an implied consent when there is continued browsing, others opt for the need to actively dismiss the banner or actively consent to the use of the cookies, which seems to be the most recommendable approach. The use of a specific cookies policy is also highly recommend and should be made available on the website, together with the privacy policy, in order to comply with the information obligations.
Data retention


The Court of Justice of the EU declared said Directive invalid in April 2014. Nevertheless, the referred Data Retention Law is still applicable, as only national courts can consider if any legislative act is valid or not.

However, this decision of the Court of Justice affects the application of the Law as national courts should not apply the rules of said Directive. Therefore, there is some apprehension as to how Portuguese legislation regarding data retention will be applied or will change.

Do not call registry

It is determined by Law for the processing of personal data and the protection of privacy in the electronic communications sector that the General Directory of Consumers is responsible for keeping an updated national list of legal persons who express their wish not to receive unsolicited communications for direct marketing purposes. However, this list is not available and it is not up to date.

Nevertheless, at the moment, companies that send this type of unsolicited communications for direct marketing purposes should keep, on their own or through representative bodies, an up-to-date list of persons who have given clearly and free of charge their consent to receive such communications, as well as of clients who did not object to the reception of the same.

3. Law Applicable


Data protection rules may also be found in the following Laws:

1. Constitution of the Portuguese Republic (available in English at http://www.cnpd.pt/english/bin/legislation/article_35.HTM);


2. Law 41/2004 of August 18, 2004 on the processing of personal data and the protection of privacy in the electronic communications sector, as modified by the Law 46/2014 of August 29, 2014 (only available in Portuguese at http://www.cnpd.pt/bin/legis/nacional/Lei_46_2012.pdf);


4. Key Privacy Concepts

a. Personal Data

Personal data shall mean any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person (“data subject”). An “identifiable person” is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

It is worth noting that data will only be considered ‘anonymous’, and therefore not ‘personal data’, provided that the individual to whom it relates cannot be identified, whether by the data controller or by any other person, taking account of all the means likely reasonably to be used either by the controller or by any other person to identify that individual.
b. Data Processing

Data Processing is defined as any operation or set of operations which is performed upon personal data, whether wholly or partly by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

c. Processing by Data Controllers

Data Protection Law applies to a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (“Controller”).

Therefore, where the purposes and means of processing are determined by laws or regulations, the controller shall be designated in the Act establishing the organization and functioning or in the statutes of the legal or statutory body competent to process the personal data concerned.

d. Jurisdiction/Territoriality

Data Protection Law shall apply to the processing of personal data carried out:

- in the context of the activities of an establishment of the controller in Portugal;
- outside Portugal, but in a place where Portuguese law applies by virtue of international public law;
- by controllers who are not established on European Union territory and who for purposes of processing personal data make use of equipment, automated or otherwise, situated on Portuguese territory, unless such equipment is used only for purposes of transit through the territory of the European Union.

Thus, Data Protection Law is applicable according to Jurisdiction criteria and independently of the nationality of the data subjects whose data are being processed.

“Establishment” shall be considered, irrespective of its legal structure, as any stable installation allowing the effective and real undertaking of an activity.

e. Sensitive Personal Data

Data Protection Law qualifies as Sensitive Personal Data any information regarding philosophical or political beliefs, political party or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, including genetic data.
As per Article 7 of the Data Protection Law, the processing of such data is permitted if:

- data subject has given his/her explicit consent for such processing;
- it is foreseen in a legal provision;
- it is essential for exercising legal or statutory rights of the controller based on important public interests grounds;
- it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent;
- it is carried out with the data subject’s consent in the course of its legitimate activities by a foundation, association or non-profit seeking body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
- it relates to data which are manifestly made public by the data subject, provided his consent for their processing can be clearly inferred from his declarations;
- it is necessary for the establishment, exercise or defence of legal claims and is exclusively carried out for that purpose.

In such case, data relative to those assessments will fall within the category of sensitive data and will be subject to specific security measures and the processing of such data subject to prior authorization from the CNPD.

Furthermore, processing of data relating to health and sex life, including genetic data, is permitted only if necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, provided those data are processed by a health professional bound by professional secrecy or by another person also subject to an equivalent obligation of secrecy and are notified to the CNPD, and where suitable safeguards are provided.

Finally, Data processing relating to suspicion of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties it is only permitted if:

- central registers to persons suspected of these activities were created and kept by public services vested with that specific responsibility by virtue of the law establishing their organization and functioning, subject to observance of procedural and data protection rules provided for in a legal order, with the prior opinion of the CNPD;
such processing is necessary for pursuing the legitimate purposes of the controller, provided the fundamental rights and freedoms of the data subject are not overriding. However it is mandatory to obtain authorization from the CNPD and to observe rules for the protection of data and the security of information.

Even though not explicitly provided for in Article 7 of the Data Protection Law, the processing of personal data relating to credit and the solvency of the data subjects is qualified as sensitive personal data and subject to a prior authorization from CNPD pursuant Article 28 of the Data Protection Law. It should also be noted that CNPD has issued Guideline 156/09 on credit information.

f. Employee Personal Data

There is no specific legal framework in the EU governing data processing in the context of employment. According to Data Protection Directive, employment relations are specifically referred to only in Article 8 (2) of the directive, which concerns the processing of sensitive data.

Notwithstanding, Employee Personal Data may include sensitive Personal Data and non-sensitive Personal Data. With regard to sensitive employee personal data, its processing is subject to the conditions stated above in paragraph (e) in accordance with number 4 of Article 17 of the Portuguese Labour Code. In addition, Articles 18, 19, 20, 21 and 22 of the aforementioned Code are also applicable, when considering the privacy of private life of the employee, such as medical examinations and biometric data.

The Portuguese Labour Code does not govern this matter in detail, only stating in Article 22 that the Employer has the right to monitor, having however to take into account the employees right of privacy. Nevertheless, the CNPD has approved official Guidelines concerning the monitoring of employees at the workplace and the procedures to be adopted by the employers.

Also with regard to sensitive employee personal data, the CNPD has approved official Guidelines on processing of personal data for preventive and curative medicine purposes regarding the control of psychoactive substances given to employees.

As per Article 6 of the Data Protection Law, non-sensitive Personal Data may be processed by a Data Controller (e.g., the employer), in particular, for the performance of a contract to which the Data Subject is a party (e.g., an employment contract), for compliance with a legal obligation to which the controller is subject or where processing is necessary for the purposes of legitimate interests of the controller to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject.
In addition, non-sensitive personal data may be processed if the data subject (e.g., the employee) has unambiguously given his consent. It is worth noting that consent as a legal basis for processing employment data must be analyzed carefully given the fact that the economic imbalance between the employer asking for consent and the employee giving consent will often raise doubts about whether consent was given in a free basis or not [see Section 5(d) below].

The CNPD has issued two exemptions concerning the prior notification requirement for data processing, regarding employment personal data. The authorizations for the exemptions set some conditions, which need to be met, in order to have the data processing exempted. The data processing exempted from notification concern the following purposes:

1. Exemption 1/99 - Processing of employees’ salaries and retributions;
2. Exemption 3/99 - Invoicing and contacts with clients, suppliers and service providers.

The CNPD has also issued several Guidelines related to the processing of employee personal data:

- Principles applicable to processing of personal data as a result of the use of geolocation devices in an employment context (2014);
- Principles applicable to the monitoring of the use of information technologies for private purposes in the workplace (2013);
- Principles applicable to processing of data with the purpose preventive and healing medicine within the scope of alcohol and drug controls performed to employees (2010);
- Principles applicable to processing of data within the scope of information management for Health and Safety Services in the workplace (2010);
- Principles applicable to processing of data with the purpose of the internal communication of irregular financial management acts – Ethics Lines (2009);
- Principles applicable to processing of biometric data for access and assiduity control (2004).

5. Consent
   a. General

According to the Data Protection Law, data subject’s consent shall mean any freely given, specific and informed indication of his wishes, by which the data subject signifies his agreement to personal data relating to him being processed.
Data Subject’s consent is one of the legitimate grounds to data processing. Thus, consent as a legal basis for processing personal data must be free, informed and specific. On the other hand, consent must be given unambiguously by acting in a way which leaves no doubt that the data subject agrees to processing of his or her data.

Moreover, there are no limitations as to how consent may be obtained: on paper with hand-written signature, electronically, via the Internet or intranet or via email. Preferably it should be in a format which can easily be reproduced as evidence.

Lastly, consent can be withdrawn at any time and there should be no requirement to give reasons for withdrawal and no risk of negative consequences over and above the termination of any benefits which may have derived from the previously agreed data use.

b. Sensitive Data

As mentioned in Section 4 (e) above, the processing of sensitive data is prohibited unless the data subject has given his/her explicit consent for such processing.

So, consent to sensitive data processing must be explicit and given in any form.

c. Minors

Under Portuguese legislation, in particular the Data Protection laws, regarding the execution of contracts by minors, it is determined that the following relevant age ranges are to be considered:

1. 0-16 – may not conclude a valid contract under Portuguese law.
2. 16-18 – equally may not conclude a valid contract under Portuguese law. However, there are some exceptions: agreements commonly concluded in small, current day-to-day activities and legal transactions related to the minor’s profession, art or occupation, where the minor was authorized to exercise or practice in the exercise of profession, art or occupation. Additionally, minors over 16 can carry out administrative acts or dispose of goods that they have acquired with the profits of their profession. Only minors above the age of 16 may be criminally liable.

The CNPD has issued an opinion where it stated that children have inter alia, the right to access data, amend it, and block it. Children also have the right to oppose the processing of their data.

However, based on the opinion (which referred to the national regulations), it seems that minors below 13 will not be able to provide a valid consent for the processing of their data. Minors aged 13 and over will be able to grant such consent, subject to a lack of opposition (their parents should be aware of the facts) from their parents (or other legal representative).
In terms of the above mentioned Guideline it is determined that “minors have the right to be informed of the processing from adolescence” and, “from a certain age, minors have legitimacy to consent to the processing of some personal data” (e.g., regarding their religious beliefs or the disclosure of information on the Internet).

In accordance with Portuguese Civil and Criminal law, we hold the opinion that only minors above 16 have such capacity, and therefore minors of said age do not have the capacity to exercise their own rights which should be supplied by parental responsibility or alternatively by guardianship.

In addition parents or legal guardians have the right to access the information once provided by the minor and to rectify or erase their personal data.

d. Employee Consent

Although Portuguese Legislation does not govern this matter in detail, the CNPD has followed the opinion of Article 29 Working Party.

The Article 29 Working Party has analyzed the significance of consent as a legal basis for processing employment data. The Working Party found that the economic imbalance between the employer asking for consent and the employee giving consent will often raise doubts about whether consent was given freely or not. The circumstances under which consent is requested should, therefore, be carefully considered when assessing the validity of consent in the employment context.

The Working Party acknowledges, however, that there will be cases where it is appropriate for an employer to rely upon consent, for example, in an international organization where employees wish to take advantage of opportunities in a third country.

e. Online/Electronic Consent

Although Portuguese Legislation does not have specific regulation on electronic consent, it is understood that consent may be given electronically. In its Opinion 15/2011 on consent, the Article 29 Working Party stated that “In the on-line environment explicit consent may be given by using electronic or digital signatures. However, it can also be given through clickable buttons depending on the context, sending confirmatory emails, clicking on icons, etc.”

Thus, online/electronic consent may be given, e.g., by clicking a button, not being required an advanced electronic signature under Article 2(2) eSignature Directive 1999/93/EC.

6. Information/Notice Requirements

As per Article 10 of the Data Protection Law, Data Subject must be informed of the following when data relating to him or herself are collected:

- the identity of the controller and of his representative, if any;
• the purposes of the processing;
• other information such as:
  ○ The recipients or categories of recipients;
  ○ Whether replies are obligatory or voluntary, as well as the possible consequences of failure to reply;
  ○ The existence and conditions of the right of access and the right to rectify, provided they are necessary, taking account the specific circumstances of collection of data in order to guarantee the data subject that they will be processed fairly.

The documents supporting the collection of personal data shall contain the information set down above.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Portuguese Law expressly provides rights to be granted in favor of data subjects. These rights include the access, rectification, cancellation and objection for the collection and treatment of personal data.

Data subjects must be informed of the existence of their right of access. In substance, any data subject has the right to obtain from the data controller:

1. Confirmation as to whether or not data relating to him or her is being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data is disclosed,
2. Communication in an intelligible form of the data undergoing processing and of any available information as to their source.

The right of access consists of the right to obtain free of charge information on his personal data, its origin and their communication.

On the other hand, data subject must be informed of additional rights.

1. Rights of rectification or cancellation: by means of these rights, the data subject may request the amendment of its data where he considers that they are inaccurate or incomplete, or even their deletion. Cancellation implies that the personal data shall be blocked and only maintained at the
disposal of Public Entities or Courts in connection with potential liabilities arising from the data processing and during relevant statutes of limitation.

2. Right of objection: data subjects have the right to request that the processing of his personal data not be carried out or ceased in certain situations, such as when the consent is not necessary or when the purpose of processing is advertising or commercial research activities.

As per the above, data subject must be informed about their right to request the rectification of inaccurate data, as well to object, at any time and for free, to the processing of their data for direct marketing purposes.

9. Registration/Notification Requirements

Data controllers are obliged to notify or to request prior authorization from the CNPD regarding personal data files. Said notification or authorization must be performed prior to the use of any file or of any data processing operation. Any change of contents of the file or its use, including its cancellation, must be communicated to the CNPD. This obligation must be performed by means of the forms available at the CNPD web page and must be sent by the data controller electronically. (http://www.cnpd.pt/bin/legal/forms.htm).

Nevertheless, there are some Exemptions to the above mentioned obligation of notification, namely the following:

1. Exemption 1/99 - Processing of employees’ salaries and retributions
2. Exemption 2/99 - Management of libraries’ and archives’ users
3. Exemption 3/99 - Invoicing and contacts with clients, suppliers and service providers
4. Exemption 4/99 - Administrative management of employees, staff and service providers
5. Exemption 5/99 - Access control (entries and exits) in buildings
6. Exemption 6/99 - Collection of quotes in associations and contacts with affiliates

The Exemptions referred above are subject to certain conditions and limitations, in order to avoid the notification obligation before the CNPD.

The notification and authorization files should be completed electronically, which requires the payment of EUR 75,00 fee and EUR 150,00 fee, respectively.

After receiving the files, the CNPD should issue a formal confirmation for the collection and processing of personal data. However, when the data controller is only requested to notify the CNPD of the collection and processing of personal data, it can automatically proceed with the data processing activities. On the contrary, when it has submitted an authorization file, the data controller
should obtain prior confirmation from the CNPD that it is possible to collect and process personal data.

The notification form requires detailed information, including the following:

1. Surname, first names and full address or legal name and registered office, phone number and email of the Data Controller;
2. Contact person of the Data Controller;
3. Processing entities;
4. The purpose, or purposes, of the processing;
5. The categories of personal data to be processed including a detailed description of the same;
6. If sensitive personal data is collected and a description of the same;
7. If personal data is communicated to third parties;
8. The manner in which data subjects are informed, to whom access requests should be submitted;
9. The period of time that personal data is stored;
10. A general description of security measures;

If the personal data is to be transferred to a foreign country, the categories of personal data to be transferred, the purposes, and the destination country to which each category of personal data may be transferred.

10. Data Protection Officers

No specific requirements apply. The appointment of a data protection officer is not regulated under Portuguese Law.

11. International Data Transfers

Transfers of personal data from Portugal to countries offering an equivalent level of protection may take place freely, if it is a country that has been recognized by the European Commission as having adequate data protection laws. Said countries are EU and EEA Member States, Argentina, Israel, Andorra, Faroe Islands, Canada, Switzerland, Guernsey, the Isle of Man, Jersey, New Zealand, Uruguay and US recipients that have signed up to the Safe Harbor arrangement, and any other countries which are deemed to grant an equivalent level of protection under a decision of the European Commission. International transfers to third countries not granting an equivalent level of protection, such as the US (except as indicated above), may only take place under the Data Protection Law where the prior authorization of the CNPD has been obtained. Exceptions to this situation are where:
1. The data subject has given their unambiguous consent to the transfer;
2. The transfer is necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken upon data subject’s request;
3. The transfer is necessary for the performance of a contract concluded or to be concluded in the interest of the data subject between the data controller and a third party;
4. The transfer is necessary for litigation purposes;
5. The transfer is in the public interest, for tax or other authorities.

The transfer of Personal Data to a non-EEA country with inadequate protection levels is also permitted with the prior authorization of the CNPD if a data transfer agreement is used and the agreement incorporates the EU model contractual clauses for the transfer of Personal Data to third countries adopted by the European Commission on 15 June 2001 and 27 December 2004 (Data Controller to Data Controller) or on 5 February 2010 (Data Controller to Data Processor).

12. Security Requirements

In order to guarantee the security of processing, the Data Controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, having regard to the state of the art and the cost of their implementation. Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

With regard to sensitive data, Data Controllers shall take the appropriate measures to:

- prevent unauthorized persons from entering the premises used for processing such data (control of entry to the premises);
- prevent data media from being read, copied, altered or removed by unauthorized persons (control of data media);
- prevent unauthorized input and unauthorized obtaining of knowledge, alteration or elimination of personal data input (control of input);
- prevent automatic data processing systems from being used by unauthorized persons by means of data transmission premises (control of use);
guarantee that authorized persons may only access data covered by the authorization (control of access);

• guarantee the checking of the entities to which personal data may be transmitted by means of data transmission premises (control of transmission);

• guarantee that it is possible to check a posteriori, in a period appropriate to the nature of the processing, which personal data are input, when and by whom (control of input);

• in transmitting personal data and in transporting the respective media, prevent unauthorized reading, copying, alteration or elimination of data (control of transport).

Furthermore, the Law 12/2005 of January 26, 2005 on Genetic and Health Information foresees the following specific security measures:

• Health information, including recorded clinical data, analysis results and other tests, interventions and diagnosis, is owned by the employee.

• The access to health information is provided by a health professional;

• Protection of confidentiality;

• Security of facilities and equipment;

• Control of the access to sensitive data.

Additionally, please also take into consideration that the CNPD has approved several official guidelines concerning processing of health and medical information, more specifically on clinical trials, clinical studies and medicinal products for human consumption.

According to CNPD the controllers and processors of such health data must observe special security measures in order to comply with specific security standards stated by the Authority. For this reason, the CNPD has established, among others, the following measures:

• Separation (physical and logical) between health data and administrative data by creating users profiles with different access levels;

• Users passwords should be frequently changed;

• Control of access to information by avoiding access by unauthorized staff;

• Encrypted transmission of health data;

• Sensitive Data backups;

• Logging of all access to health information.
Finally, in what concerns the processing of personal data and the protection of privacy in the electronic communications sector, companies providing electronic communication services must take technical and organizational appropriate measures in order to guarantee the security of their services, such as:

- Ensure that only authorized staff have access to personal data;
- Protect personal data against destruction, loss, alteration, disclosure or unauthorized access;
- Ensure the implementation of a safety policy in the processing of personal data.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

It is possible the Data Controller entrusts the processing of personal data to a processor. In what concerns the processing of personal data by third party processor, the Data Controller must choose a processor who is capable of offering sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

The controller is defined as the one who determines the purposes and means of the processing of personal data. If this power is delegated to a third party processor, the controller must be able to interfere with the decisions of the processor regarding the means of processing. Thereafter, the relationship between controller and processor, i.e., the carrying out of processing by way of a processor, must be governed (i) by a written contract or legal act binding the processor to the controller, (ii) the processor shall act only on instructions from the controller and (iii) the processor must comply with the security measures as foreseen in Portuguese Legislation.

In addition, an equal obligation must be observed by any person acting under the authority of the controller or the processor, including the processor himself, who has access to personal data, who not process them except on instructions from the controller, unless he is required to do so by law.

14. Enforcement and Sanctions

Civil and criminal penalties, as well as private rights of action can be applicable.

The CNPD has the power to investigate complaints and cases, and to order the suspension of processing and/or transfer of data, as well as the destruction of data and other similar actions including administrative fines; these orders can be appealed to the courts.
Individuals can file complaints with the CNPD, and can seek a judicial remedy for violations of the law. As the Data Protection Law can be applicable, fines ranging from EUR 250,00 to EUR 2,500,00 in the case of natural persons and fines ranging from EUR 1,500,00 to EUR 15,000,00 in the case of legal persons; and imprisonment of up to 1 year, for the breach of data protection laws can be imposed.

The above fines may be increased to double the amount [i.e., EUR 500,00 and up to EUR 5,000,00 in the case of natural persons, and EUR 3,000,00 up to EUR 30,000,00 in the case of legal persons] if referring to the requirements of sensitive data or data subject to prior authorization. In this case, it is also possible to be subject to imprisonment of up to 2 years.

Also, the infringement of the access to the personal information storage is punishable with a fine ranging from a minimum of EUR 1,500,00 and a maximum of EUR 25,000,00, when the offender is an individual, and from a minimum of EUR 5,000,00 and a maximum of EUR 5,000,000,00, when it is the legal entity that breaches the duty (according to paragraph 1, of Article 14, of Law No 41/2004, August 18).

Finally, Directors and individuals within a company may also face legal sanctions, for the breach of data protection laws.

15. Data Security Breach

In Portugal, the only data breach notifications that are legally required concern electronic communication providers.

As per Article 3-A of the Law 41/2004 of August 18, 2004 on the processing of personal data and the protection of privacy in the electronic communications sector, as modified by the Law 46/2014 of August 29th, 2014, if there is a risk that the breach will negatively affect the personal data, the subscriber or individual whose data could be affected must be notified by the electronic communications service provider.

This notification obligation will not apply if the companies offering publicly available electronic communications services are able to prove to the CNPD that they have taken the necessary technological protection measures and that these measures were applied to the data breached.

This legal disposition also requires companies that offer electronic communication services to notify the CNPD whenever there is a personal data breach.

Whenever the CNPD verifies the infringement of any duty or obligation, it shall notify the offender of such fact and give him/her the opportunity to respond within a minimum period of 10 days and, if appropriate, to end the non-compliance.
The infringement with the notification duty amounts to an administrative offense punishable with a fine ranging from a minimum of EUR 1,500.00 and a maximum of EUR 25,000.00, when the offender is an individual, and from a minimum of EUR 5,000.00 and a maximum of EUR 5,000,000.00, when it is the legal entity that breaches the duty.

The non-compliance with the notification requirements is punishable with a fine ranging from a minimum of EUR 500.00 and a maximum of EUR 20,000.00, when the offender is an individual, and from a minimum of EUR 2,500.00 and a maximum of EUR 2,250,000.00, when it is the legal entity that breaches the duty.

16. Accountability

Accountability requires the active implementation of measures by controllers to promote and safeguard data protection in their processing activities. Similar information is foreseen in number 2 of Article 5 of the Data Protection Law in which the controller shall ensure that personal data is processed accordingly with the rules established therein.

In accordance with the Article 29 Working Party’s opinion, the essence of accountability is the controller’s obligation to:

- Put in place measures which would – under normal circumstances – guarantee that data protection rules are adhered to in the context of processing operations;
- Have documentation ready which proves to data subjects and to supervisory authorities what measures have been taken to achieve adherence to the data protection rules.

The principle of accountability requires controllers to actively demonstrate compliance and not merely wait for data subjects or supervisory authorities to point out shortcomings.

17. Whistle-Blower Hotline

The CNPD issued Guidelines 765/2009 for data processing in the context of whistle-blower hotlines, namely its implementation and how to proceed. This type of data collection and processing is applicable to personal data related to accounting, internal accounting controls and auditing matters. The hotline may be used against bribery, banking and other financial crimes.

Although not expressly provided for in Article 7 of the Data Protection Law, the processing of personal data relating to whistle-blower hotlines is qualified as sensitive personal data pursuant Article 8 of the same Law and for that purpose it is subject to prior control and authorization from the CNPD.
The authorization file should specify in detail the legitimacy and the need for the proposed processing, and data controllers must inform their employees about the existence of the whistleblower hotline and how they can use it, for example by means of a Privacy Police of the company.

The following categories of data are considered sufficient:

1. Identity and professional category of the whistleblower;
2. Identity and professional category of the denounced;
3. Identity and professional functions of the people that collect and process personal data;
4. The facts that are included in the suspicious activities;
5. The elements collected regarding the investigation procedure;
6. The whistle blower purpose.

18. E-Discovery

The implementation of an e-discovery system within an organization whereby employers are entitled to monitor equipment (phone calls, email and Internet access) used by employees in their professional activities raises issues regarding the right of privacy and the right to the secrecy of communications.

Pursuant to Articles 26 and 35 of the Constitution of the Portuguese Republic, all citizens have the right of privacy and the right of protection of their own personal data. On the other hand, the secrecy of communication is established in Articles 32 and 34 of the Constitution of the Portuguese Republic and in Article 194 of the Portuguese Criminal Code in which any intrusion in communications is punishable as a crime.

Other rules regarding this subject may be found in Article 80 of the Portuguese Civil Code and in the Portuguese Labour Code.

Furthermore, the CNPD has approved Guidelines regarding the monitoring of employees in the workplace. These Guidelines have stated the general principles:

- The employer shall – before starting any kind of processing – inform the employee about the conditions, under which equipment belonging to the corporation may be used for private purposes and the level of tolerance admitted; the existence of the processing, its purpose, the control methods adopted, the data processed and its storage, as well as the consequences for the misuse of the communications equipment made available to the employee.
• The data processing and the means of control shall be adequate to the business management, to the development of the productive activity and be compatible with the rights and duties of the employees, and must not be abusive or disproportionate in relation to the level of protection of the employee’s private sphere.

• The employer shall use generic monitoring methodologies.

In order to comply with the constitutional rights described above, the CNPD established the following procedures to be adopted by the employers:

1. The level of private use allowed on equipment issued to the employee by the corporation, the conditions for data processing and the definition of the forms of monitoring adopted shall be included in the internal Rules of Procedure (“RoP”), which shall be submitted to the workers council for their opinion.

2. The employer shall disclose the content of the RoP, namely by posting it in the corporation’s headquarters and in all other working places, in order to allow the employees to have full knowledge of it.

3. The employer, as data controller, has to request authorization from the CNPD to conduct data processing, enclosing the RoP in the process and specifying the ways used to disclose the conditions of the data processing to the employees.

19. Anti-Spam Filtering

Although there are no specific laws that regulate the use of anti-spam filtering, in general terms and to the extent that the use of an anti-spam filtering solution will involve the use of an organization’s email system for data processing, the referred anti-spam filtering will have to be authorized by the CNPD and will have to comply with data protection laws.

Also, it is necessary to inform employees of the monitoring of their emails, namely by referring the purpose of the spam filtering solution and which entities will process the information contained in the same.

20. Cookies

The use of cookies should comply with data protection laws and, therefore, the cookie consent requirement set forth by Directive 2009/136/EC, amending ePrivacy Directive 2002/58/EC, was implemented into Portuguese jurisdiction by Law 46/2012 on August 29, 2012 which amended Law 41/2004 of August 18 concerning the processing of personal data and the protection of privacy in the electronic communications sector, which determined that:

1. The storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user shall only be allowed on condition that the subscriber or user concerned has given his
or her consent, having been provided with clear and comprehensive information about the purposes of the processing;

2. The data controller must give users the possibility to withdraw their consent freely and in an easy manner.

3. Nevertheless, the consent requirement does not prevent any technical storage or access of data:
   a) For the sole purpose of carrying out the transmission of a communication over an electronic communications network;
   b) As strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

21. Direct Marketing

For direct marketing purposes, Law 46/2012 of August 29, 2012 which amended Law 41/2004 of August 18 concerning the processing of personal data and the protection of privacy in the electronic communications sector, which determined that:

1. The sending of unsolicited communications for direct marketing purposes, namely the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines or electronic mail, including SMS (Short Message Service), EMS (Enhanced Message Service) and MMS (Multimedia Message Service) and other kinds of similar applications, are subject to the prior and explicit consent of a subscriber;

2. A provider of a certain product or service, that obtained from its customers their electronic contact details, in the context of the commercial relationship or of the service provided, can use such electronic contact details for direct marketing purposes for the service provider’s own similar products or services; however, customers should be clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details:
   a) At the time of their collection; and
   b) On the occasion of each message, in case the customer has not initially refused such use.

3. It is prohibited to send electronic mails for the purpose of direct marketing if it disguises or conceals the identity of the sender on whose behalf the communication is made, particularly if it does not have a valid address to which the recipient may send a request to stop receiving communications or which encourage recipients to visit websites that are contrary to the purposes of data protection.
Russia

Edward Bekeschenko
Moscow
Tel: +7 495 787 2700
edward.bekeschenko@bakermckenzie.com

Ekaterina Kobrin
Moscow
Tel: +7 495 787 2700
ekaterina.kobrin@bakermckenzie.com

Dmitry Lysenko
Moscow
Tel: +7 495 787 2700
dmitry.lysenko@bakermckenzie.com

Evgeny Reyzman
Moscow
Tel: +7 495 787 2700
evgeny.reyzman@bakermckenzie.com
1. Recent Privacy Developments

*Databases Localization Requirements*

The new “localized database” requirement introduced by the Federal Law No. 242-FZ provides that starting from 1 September 2015, the operators collecting personal data shall ensure the recording, systematizing, accumulating, storing, verifying (including updating and modifying) and retrieving of personal data of citizens of the Russian Federation using databases located on the territory of the Russian Federation. The definition of the operator relevant for this purposes is very general and covers both local and foreign operators collecting data of Russian citizens.

This requirement is subject to several narrowly defined exceptions. For example, an exception applies if processing personal data is necessary for compliance with other legal requirements or for the conduct of scientific work.

Because the language of the requirements is unclear in all matters except for the possibility to have databases outside Russia, there been suggestions that it is sufficient to duplication/mirror data bases and various manners to identify Russian citizens and how data already outside of Russia are to be treated have been discussed. As per March 2015, there has not been a clarification on this issues. Rather, the regulator has recently stated it would be holding face-to-face consultations with the market-leading data operators in the IT and services industries in order to arrive at some practical solutions for the compliance with the law.

*Blocking Websites for Data Processing Violations*

Federal Law No. 242-FZ also introduced a procedure for blocking websites through which personal data are processed in violation of the law.

Accordingly, the violating website is to be registered as being in violation if a relevant court decision exists. After registration, the owner is to be notified, asked to cure the violation and in case of failure to do so the provider is required to block the website.

Similarly to the discussion on the requirements of the law, there are differing views on issues such as the requirements for the blocking are in case different IP services or dynamic IP technologies, with the regulator having made statements to the effect that it would apply the most encompassing implementation options.

Also, the authority of the regulator to conduct inspections relating to data processing rules and exchange of data in Internet has been extended, and the restrictions relating to frequency and length of inspections and prior notification available under Federal Law No. 294-FZ to safeguard the interests of business have been waived.
2. Emerging Privacy Issues and Trends

**Increase of fines for data protection violations** - the Russian parliament is currently reviewing the draft bill aiming to increase the fine for personal data protection violations to up to 300,000 rubles (currently slightly less than 50,000 USD).

3. Law Applicable

The Russian legal regime governing the collection and processing of Personal Data is principally set out in the Federal Law on Personal Data (the “**Personal Data Law**”) of July 27, 2006 (as amended).

Chapter 14 of the Russian Labor Code also regulates the treatment of employee’s personal data.

A number of other laws contain more specific provisions on Personal Data treatment; however, such regulations are based on the same principles as the Personal Data Law.

4. Key Privacy Concepts

a. **Personal Data**

The Personal Data Law defines “Personal Data” to mean any data related to a directly or indirectly identified or identifiable individual (“Personal Data Subject”), including his or her first name, middle name and last name, year, month, date and place of birth, marital and social status, welfare, education, profession, income etc. Under the Labor Code (where a separate definition is given), Personal Data is defined as data on a particular employee that is needed by the employer in connection with the employment relationship (together “Personal Data”).

b. **Data Processing**

Under the Personal Data Law, Personal Data processing has been defined very broadly, as any action (operation) or aggregation of actions (operations) with Personal Data, performed with or without computer equipment, including collection, recording, systematization, accumulation, storage, verification (updating and amending), extraction, use, transfer (dissemination, granting, depersonalization, blocking, deletion and destruction of Personal Data. Under the Labor Code, employees’ Personal Data processing is defined as the collection, storage, combination, transmission, or any other use of Personal Data.

Russian data protection legislation regulates both manual and automated data processing. Neither the Personal Data Law nor the Labor Code distinguishes among various types of data processing, except that they prohibit Data Controllers and other parties from relying solely on automatically processed data in making legally binding decisions with respect to Personal Data.
Subjects, including employees, unless their consent is obtained. Also, manual data processing does not require notification to the competent authority.

c. **Processing by Data Controllers**
The Personal Data Law regulates general and specific issues related to processing of Personal Data by state and municipal bodies, private legal entities and individuals, which are engaged in the processing of Personal Data (“Data Controllers”). The Personal Data Law determines major principles of Personal Data processing. Personal Data may be processed by Data Controllers only with the consent of Personal Data Subjects. The consent is not required in a number of cases explicitly stated in the Personal Data Law. Data Controllers must ensure confidentiality of Personal Data, unless otherwise provided for by the Personal Data Law. The Labor Code also expressly determines the purposes for which, and the procedure pursuant to which, Personal Data of an employee is to be processed by Data Controllers.

The Personal Data Law does not distinguish between Data Controllers and Data Processors; however, it stipulates that Data Controllers may engage service providers for processing of personal data on the basis of a contract which must contain substantial non-disclosure provisions.

d. **Jurisdiction/Territoriality**
Relevant Russian laws do not specify the territory covered by them. The laws apply to protect Personal Data and rights of Personal Data subjects irrespective of the origin of the Data Controllers.

e. **Sensitive Personal Data**
As a general rule, the processing of certain categories of Personal Data, which include data on individual’s political, religious, philosophic or other beliefs, race and national identity, state of health and private life (“Sensitive Personal Data”) is restricted. The Personal Data Law allows processing of Sensitive Personal Data only in a limited number of cases explicitly stated in the Personal Data Law. For instance, processing of Sensitive Personal Data is allowed if the Personal Data Subject has agreed to such processing in writing, or if this Personal Data is processed by medical professionals for medical purposes, or the processing is required for execution of justice, criminal prosecution and other cases specifically referred to in the Personal Data Law. Under the Russian Labor Code, Sensitive Personal Data may be processed by the employer only upon written consent of the employee and if such processing is required for the purposes of resolving a matter directly related to the employment relationship. An employer may not seek or process Personal Data of an employee with respect to the employee’s affiliation with a non-governmental entity or trade union activities except in cases expressly provided for by law.
There are special restrictions on the processing of data regarding personal physiological and biological parameters by which an individual can be identified (“Biometric Personal Data”). Under the Personal Data Law such Biometric Personal Data may be processed by Data Controllers only with a written consent of Personal Data Subjects. The consent of a Personal Data Subject is not required if the data is processed for the purposes of execution of justice, criminal investigation, and other cases explicitly stated in applicable Russian legislation.

It is expressly prohibited by the law to process data related to a person’s criminal record other than by authorized state bodies for the designated purposes.

f. Employee Personal Data
Employee Personal Data is likely to include Sensitive Personal Data (e.g., health-related information) and non-sensitive Personal Data. Sensitive Personal Data may be processed in the circumstances mentioned in Section 4(e) above and, in particular, if an employee wishes to observe a religious holiday not officially recognized in Russia as a public holiday. Non-sensitive Personal Data of employees provided in connection with employment may be processed by the employer. An employer should obtain employees’ Personal Data only from the employees, unless the employees give their consent in writing to obtain data about them from third parties.

5. Consent
a. General
Consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data, except in certain prescribed circumstances. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous.

Consent is contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

When the Data Subject gives consent, it is understood to only cover the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

There are generally no specific requirements for the form or manner in which consent must be obtained from Data Subjects but in some cases consent must be in writing. Consent has to be specific, informed and conscious.

In addition, the Data Subject also has the right to withdraw consent at any time.
b. Sensitive Data
Russian law recognizes Sensitive Data as a special category of Personal Data. It is subject to additional and special consent requirements. While Sensitive Data may only be collected and processed upon written consent of the Data Subject, Sensitive Data may be processed without obtaining consent in certain prescribed circumstances.

Consent is not required for processing of Sensitive Personal Data, including Biometric Personal Data: by medical professionals for medical purposes, or if Personal Data is made publicly available by the Personal Data Subject, or if processing is required for the execution of justice, criminal prosecution, and other cases as stated in the Personal Data Law.

c. Minors
While consent from minors is not specifically addressed in any law, the general rule is that minors are considered incapable of giving consent. However, parents or legal guardians of minors are allowed to provide consent on behalf of the minor, and may even be allowed to obtain information about the minor from third parties without the need of consent from the minor.

d. Employee Consent
In Russian law, there are doubts as to whether consent given in the context of an employment relationship can be considered valid given that the employee may feel forced to consent due to the subordinate nature of their relationship with their employer.

The general rule is that employee consent is required to collect and process an employee’s Personal Data; however, there are instances when employee consent is not required, e.g., to carry out an employment contract or administer an employment relationship, or to fulfill a legitimate interest of the employer.

e. Online/Electronic Consent
As stated in Section 5(a), nothing in Russian law prohibits the use of electronic consent, except where written consent is expressly required. Proof of the fact that the consent was signed by the proper (authorized) person will be the electronic signature on the consent (which must be in accordance with legislation regulating electronic signature).

6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity, the types of Personal Data being collected; purposes for collecting Personal Data, its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be
transferred; where the Personal Data is to be stored; how to contact the privacy officer or the person accountable for the organization’s policies and practices; how to make an inquiry or a complaint; how to access and/or correct the Data Subject’s Personal Data; the duration of the proposed processing; and the means of transmission of the Personal Data.

7. Processing Rules
An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. Registration/Notification Requirements
Before a Data Controller commences processing Personal Data, it must file with the competent state authority responsible for Personal Data protection (currently - Federal Service for Supervision Over Communications, Information Technology and Mass Communications) a notification of its intention to process Personal Data. The notice may be submitted online at the Personal Data Portal of the competent agency (http://www.pd.rsoc.ru/operators-registry/notification/). The notice may also be sent by regular mail. The notification must contain the details of the Data Controller, categories of data and Data Subjects, time period of Data Processing, legal grounds, purpose and methods of the Data Processing, and security measures applied. A person responsible for Data Processing must be appointed by the Data Controller and notified to the competent authority. The information about the Data Controllers and data processed by them is publicly available.

The notification does not have to be extremely specific and may state the required information in rather general terms.

There are certain exceptions from the notification obligation. For instance, employers are expressly exempted from the notification obligation; also, no notification is necessary when only the names, patronymics and surnames are processed or when processing of data is for the purpose of execution of the contract with the Data Subject.
10. Data Protection Officers
In Russia, organizations are required to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization. In addition, such data privacy officer or other individual must be located in Russia.

11. International Data Transfers
Organizations may transfer Personal Data outside of Russia provided that the receiving jurisdiction provides a similar level of protection for Personal Data; the affected Data Subjects have been informed or have provided consent; and reasonable steps have been taken to safeguard the Personal Data to be transferred. Furthermore, international data transfers will be considered valid provided that appropriate data transfer agreements (i.e., Model Contractual Clauses) or other prescribed measures are put in place.

12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. In case of an occurrence of data breach, the outsourcing organization may be held liable together with the third party provider.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, or criminal proceedings.

15. Data Security Breach
Organizations that are involved in a data breach situation are required to comply with mandatory data breach notification requirements; notify affected Data Subjects depending on the nature and scope of the breach; gather information about the breach, assess the potential risk of harm to the Data Subjects, take steps to contain the breach and prevent future similar breaches; assist authorities with any investigation relating to the breach; and comply with data authority orders and court orders.
Depending on the nature and scope of the breach, the organization may be required to notify the data authority.

An organization that is involved in a data breach situation may be subject to a suspension of business operations, an administrative fine, penalty or sanction, or civil actions and/or class actions.

16. Accountability

In Russia, organizations are required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data; furnish the results of the privacy impact assessments to privacy regulators upon request; and furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

17. Whistle-blower hotline

There are no laws/rules that regulate whistle-blower hotlines in Russia.

18. E-discovery

There are no laws/rules that regulate the implementation of an e-discovery system in Russia.

19. Anti-Spam Filtering

There are no laws/rules that regulate the implementation of an anti-spam filter solution in Russia.

20. Cookies

There are no laws/rules that regulate the use and deployment of cookies in Russia.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.
Saudi Arabia

Judes Abboud
Dubai
Tel: + 971 442 30080
judes.abboud@bakermckenzie.com

Haifa Bahaian
Riyadh
Tel: + 966 11 265 8900, Ext. 8968
haifa.bahaian@bakermckenzie.com

Aisha Gondal
Riyadh
Tel: + 966 11 265 8900, Ext. 8913
aisha.gondal@bakermckenzie.com

George Sayen
Riyadh
Tel: + 966 11 265 8900, Ext. 8911
george.sayen@bakermckenzie.com
1. Recent Privacy Developments

There are no specific laws or regulations in Saudi Arabia that prescribe or control the collection, storage or transfer of personal data. However, there are certain rights of privacy under various laws which provide for privacy in certain aspects including but not limited to, an individual's financial and personal information, and the privacy and confidentiality of telephone calls and information transmitted or received through public telecommunications networks, unless otherwise provided for by statute or royal decree.

While we are not aware of any legal regime that specifically controls data privacy, it should be noted that Saudi courts may use general notions of fairness to resolve any dispute related to matters of privacy and may rely on general principles of Shariah (Islamic Law).

The following is a list of laws and regulations which discuss certain rights of privacy in certain sectors in Saudi Arabia:

<table>
<thead>
<tr>
<th>Applicable Laws</th>
<th>Links</th>
</tr>
</thead>
</table>
2. Emerging Privacy Issues and Trends

*Electronic Signatures*

Electronic signatures are regulated under the Electronic Transactions Law which provides that a Certification Service Provider ("CSP"), which is a person licensed to issue digital certificates or perform any other service or task related thereto and to electronic signatures in accordance with the law, shall maintain, along with his staff, the confidentiality of information obtained in the course of business, excluding information that certificate holders permit – in written or electronic form– to be published or disclosed, or as provided for by law.

Nonetheless, a certificate holder shall be responsible for the integrity and confidentiality of his own electronic signature system, and any use of such system shall be deemed originated by him. And any person relying on an electronic signature of another person shall exercise due diligence in verifying the authenticity of the signature, using relevant electronic signature verification data in accordance with the procedures set forth by the law.

Staff of the Ministry of Communications and Information Technology, Communications and Information Technology Commission and the National Center for Digital Certification shall maintain the confidentiality of information relating to CSPs or clients thereof, obtained in the course of their work and may not disclose such information for any reason, except in cases provided for by law.

When the activities of a CSP cease to exist, the obligation of confidentiality continues as the law obligates the CSP to deliver all information and documentation in its possession to the Communications and Information Technology Commission, to be disposed of in accordance with the provisions and standards provided for in the Electronic Transactions Regulations.

*Cybercrime/ Cybersecurity*

In 2007, Saudi Arabia issued the Anti-Cyber Crime Law to regulate cyber crimes taking place in Saudi Arabia. The law aims to enhance the security of information and to protect the confidentiality and privacy of personal data.

The law defined “data” as information, commands, messages, voices, or images which are prepared or have been prepared for use in computers. This includes data that can be saved, processed, transmitted, or constructed by computers, such as numbers, letters, codes, etc. The unauthorized access to personal data is defined by the law as the deliberate, unauthorized access by any person to computers, websites, information systems, or computer networks.
The law provides a variety of sanctions and penalties for wrongfully accessing or disclosing personal data. The sanctions of violating personal data depend on the severity of the violation. The following are, amongst others, the sanctions related to each category of cyber crimes against personal data as provided by the law:

1. The act of spying on, interception or reception of data transmitted through an information network or a computer without legitimate authorization is punishable by imprisonment for a period not exceeding one year and a fine not exceeding five hundred thousand riyals or either;

2. The act of the unlawful access to bank or credit data is punishable by imprisonment for a period not exceeding three years and a fine not exceeding two million riyals; and

3. The act of the unlawful access to computers with the intention to delete, erase, destroy, leak, damage, alter or redistribute private data is punishable by imprisonment for a period not exceeding four years and a fine not exceeding three million riyals.

The competent court may exempt an offender from such punishments if the offender informs the competent authority of the crime prior to its discovery and prior to the infliction of damage. If the culprit informs the competent authority after the occurrence of the crime, the exemption from punishment shall be granted if the information he provides eventually leads to the arrest of the other culprits and the seizure of the means used in the perpetration of the crime.

3. Law Applicable

As stated above, there are no specific laws or regulations in Saudi Arabia that prescribe or control the collection, storage or transfer of personal data. Nonetheless, the laws mentioned in section 1 are the main sources of law that regulate certain aspects of privacy in different sectors in Saudi Arabia.

4. Key Privacy Concepts

a. Personal Data

“Personal data” is not defined in any laws or regulations in Saudi Arabia. Nonetheless, the privacy of personal data has been regulated in different areas under Saudi laws. The following are the laws and regulations addressing the privacy and protection measures of personal data:

Shariah

Under Shariah, there is no specific data protection regime. However, the wrongful disclosure of a person’s private information by a person to whom it has been entrusted for a specific purpose, may, in proper circumstances, create a cause of action for damages: for example, in a case where the
information is of an extremely sensitive nature and potentially slanderous, or where its negligent disclosure or loss, perhaps through inadequate data security measures, would cause direct damages to an individual.

As an example, an employer may be liable for disclosing information to the public that would damage an employee’s reputation. However, the collection and use of the information for legitimate employment purposes and retained in confidence would not ordinarily be actionable.

**Law of Civil Affairs**

This law provides that civil registers contents (including all personal data therein such as a person’s name, date of birth, ID number, and that person’s picture) are considered confidential; and it shall not be permissible to move such registers out of the Civil Affairs Departments and offices whatsoever the case; except if required otherwise by a judicial authority or an official investigation authority.

**Telecommunications Regulations**

The Telecommunications Regulations generally prohibit the disclosure of a customer’s personal information without his/her consent. In particular, Article 58 requires a service provider to operate its telecommunications facilities and telecommunications network with due regard for the privacy of its users, except as permitted or required by law, or with the consent of the person to whom the personal information relates. A service provider shall not collect, use, maintain or disclose user information or user communications for any purpose.

**Anti-Cyber Crime Law**

The Anti-Cyber Crime Law protects the confidentiality and privacy of personal information. (please refer to section 2 (Cybercrime/ Cybersecurity)).

**Regulations for Consumer Credit**

Personal data obtained from consumers, guarantors or any other person in connection with the execution and management of agreements must be kept confidential. Such consumer data may be processed only for the purpose of assessing the financial situation of the borrowers or guarantors and their ability to repay the agreed credit.

The Saudi Credit Bureau operates a central database for the purpose of registration and maintenance of credit information of consumers and guarantors. Personal data received may be processed only for the purpose of assessing the financial situation of the consumer and the guarantor and their ability to repay.
Banking Consumer Protection Principles

These Principles apply to the activities of banks operating by way of a license and under the supervision of the Saudi Arabian Monetary Agency (“SAMA”), and who are dealing with persons who are, or may become consumers. It also applies to the activities of any third party engaged by the banks for outsourced activity.

The 6th principal is the Principle of Protection of Privacy, which means that the consumers’ financial and personal information should be protected through appropriate control and protection mechanisms. These mechanisms should define the purposes for which the data may be collected, processed, held, used and disclosed (especially to third parties).

The Principles states an obligation and responsibility on banks to protect consumer data and maintain the confidentiality of the data, including when it is held by a third party. Banks are also required to provide a safe and confidential environment in all of its delivery channels to ensure the confidentiality and privacy of consumer data, and to have sufficient procedures, system controls and checks and employee awareness to protect consumer information and to identify and resolve any causes of information security breaches. Also, a bank has to ensure that the personal information of consumers can be accessed and used by authorized employees only. This is to ensure that access to consumer’s financial and/or personal information is for authorized employees only, whether on the job or after they have ceased working with the bank.

Insurance Market Code of Conduct Regulation

Insurance companies must, at all times, ensure that customer personal data is protected. This means that the data must be obtained and used only for specified and lawful purposes, kept by the insurance company in Saudi Arabia, provided to the customer upon his/her written request and not disclosed to any third party without the prior authorization of SAMA. When dealing with third parties, insurance companies must set up data confidentiality agreements before initiating a business relationship.

The regulations also protect information collected through a website, as insurance companies must ensure the confidentiality of all information collected through its website and not disclose such information to any party without the written approval of SAMA. Furthermore, it is the responsibility of the insurance company to establish appropriate procedures and controls to secure the confidentiality of information.

Insurance Intermediaries Regulation

Intermediaries shall ensure that clients data and confidential documents are stored safely with restricted access. Intermediaries are also required to treat all data and information acquired about the insurance company and clients
with utmost confidentiality, and take appropriate measures to maintain the secrecy of confidential documents in their possession. This means that the data must be obtained and used only for specified and lawful purpose, kept secure and up-to-date, and not disclosed to any third party without prior authorization from SAMA.

b. Processing by Data Controllers
Since there are no laws in Saudi Arabia that regulate or control data privacy, the concept of data controllers does not exist yet and is not defined in any laws or regulations in Saudi Arabia.

5. Consent
a. General
Under the Electronic Transactions Law, it is a criminal offence to use an applicant’s information for purposes other than for certification without the applicant’s consent in written or electronic form. CSPs can only obtain an applicant’s personal information, directly or indirectly, with that applicant’s written consent. However, the law does not outline the required content of the consent. It is also unclear whether electronic consent is sufficient for the purpose of collecting data. The law is silent on whether or not it applies to implied or inferred consent or consent by minors.

Also, as mentioned in Section 4(a) above, Telecommunications Regulations generally prohibit the disclosure of a customer’s personal information without his/her consent, except as permitted or required by law.

6. Information/Notice Requirements
There are no specific laws or regulations that we are aware of that regulate information/notice requirements in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

7. Processing Rules
There are no specific laws or regulations that we are aware of that regulate processing rules in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

8. Rights of Individuals
There are no specific laws or regulations that we are aware of that regulate rights of individuals in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.
9. Registration/Notification Requirements

There are no specific laws or regulations that we are aware of that regulate registration/notification requirements in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

10. Data Protection Officers

There are no specific laws or regulations that we are aware of that regulate data protection officers in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

11. International Data Transfers

There are no specific laws or regulations that we are aware of that regulate international data transfers in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

12. Security Requirements

There are no specific laws or regulations that we are aware of that regulate security requirements in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

13. Special Rules for Outsourcing of Data Processing to Third Parties

There are no specific laws or regulations that we are aware of that regulate outsourcing of data processing to third parties in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

14. Enforcement and Sanctions

The Banking Control Law imposes penalties on bank employees in cases of violation to the confidentiality of information possessed by such employees while performing their duties. Violators shall be liable to imprisonment for a term not exceeding two years and a fine not exceeding SAR 20,000 or either of the two penalties.

The Anti-Cyber Crime Law imposes penalties and fines that vary from SAR 500,000 to SAR 3,000,000 and imprisonment period from one year to five years. (please refer to Section 2, Cybercrime/ Cybersecurity)

The Electronic Transactions Law imposes violators to fines not exceeding SAR 5,000,000 and imprisonment for a period not exceeding five years, or both penalties.
In 2007, a spokesman for the Communications and Information Technology Commission has issued a stern warning to companies that send unsolicited SPAM messages to customers, stating that such companies could face fines of up to SAR 5,000,000 or even a cancellation of their business license.

The Telecommunications Law does not specify a penalty for violations of privacy, but it has set up a violations committee which has the jurisdiction to hear and decide on all matters relating to such violations. No other sanctions or penalties are discussed in the relevant laws.

15. Data Security Breach

There are no specific laws or regulations that we are aware of that regulate data security breach in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

16. Accountability

There are no specific laws or regulations that we are aware of that regulate accountability in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

17. Whistle-blower Hotline

There are no specific laws or regulations that we are aware of that regulate whistle-blower hotlines in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

18. E-discovery

There are no specific laws or regulations that we are aware of that regulate e-discovery in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

19. Anti-Spam Filtering

a. Definition of Spam under Saudi Law

The Regulation for Reduction of SPAM issued pursuant to the Communications and Information Technology Commission resolution number 259/1431 dated 28 March 2010 defines SPAM as any electronic message transmitted without the prior consent of the recipient through various communication modes including, but not limited to, e-mails, SMS, MMS, fax and Bluetooth.

b. Control Measures

The Regulation for Reduction of SPAM provides a number of rules to control electronic message transmissions. The Regulation prohibits any person from sending or causing to send electronic messages except if the recipient has given a prior consent to receive such messages or there exists a prior
commercial or business relationship between the sender and the recipient. Also, the electronic messages must include the name and address of the sender and the subject of the message in order to enable the recipient to send a request to cancel the subscription if they no longer want to receive such messages. Once a request has been sent, the sender would be prohibited from sending any messages after 48 hours of such request.

It should be noted that the Regulation specifically prohibits sending messages to electronic addresses obtained by automatic systems that use methods of combining names, letters, numbers, punctuation marks or symbols and prohibits the use of any computer software used for searching the internet for gathering email addresses.

c. Duties and Responsibilities of Service Providers

Certain duties and responsibilities are imposed on licensed internet service providers and mobile service providers, that such providers shall on a continuous basis, take effective measures to make their subscribers aware of these controls, the importance of the compliance therewith, and the consequences of the violation thereof.

d. Applicability of Controls

The controls are applicable to all electronic messages originated from inside the Kingdom of Saudi Arabia. International conventions shall apply on messages originated from outside the Kingdom.

Any person who is exposed to SPAM may file a complaint within 30 days from the date of receipt of the SPAM.

20. Cookies

There are no specific laws or regulations that we are aware of that regulate cookies in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.

21. Direct Marketing

There are no specific laws or regulations that we are aware of that regulate direct marketing in Saudi Arabia. It should be noted that Saudi Regulatory authorities often issue circulars and decisions that are not publicly available.
Singapore

Ken Chia
Singapore
Tel: +65 6434 2558
ken.chia@bakermckenzie.com

Quan Nguyen
Singapore
Tel: +65 6434 2592
quan.nguyen@bakermckenzie.com
1. Recent Privacy Developments

**Personal Data Protection Act comes into effect in 2014**

The Personal Data Protection Act (Act 26 of 2012) ("PDPA") was passed by the Singapore Parliament on 15 October 2012. The PDPA establishes a baseline data protection framework that applies to all organizations in the private sector. The PDPA also seeks to establish a national Do Not Call ("DNC") registry, which is intended to provide individuals with a simple and efficient way to opt-out of receiving certain unsolicited marketing messages.

The requirements associated with the implementation of the DNC registry came into force on 2 January 2014, while the substantive data protection obligations came into force on 2 July 2014.

**Personal Data Protection Regulations 2014**

On 2 July 2014, the Personal Data Protection Regulations ("PDPR") came into force. The PDPR expands on, amongst other things, the PDPA’s Access and Correction Obligation and Transfer Obligation.

In particular, the PDPR requires organizations to respond to each access request as accurately and completely as necessary and reasonably possible and within 30 days of such request being made. However, if an organization is unable to comply with this requirement, it must (within the 30 day period) inform the applicant in writing of the time by which it will respond to the request.

Further, as discussed below, the PDPR requires an organization transferring Personal Data (please refer to definition in Section 4 below) outside Singapore to take appropriate steps to ascertain whether, and to ensure that, the recipient of the Personal Data in that country or territory outside Singapore is bound by legally enforceable obligations to provide to the transferred Personal Data a standard of protection that is at least comparable to the protection under the PDPA.

**Advisory Guidelines**

The Personal Data Protection Commission ("PDPC") is tasked with the administration and enforcement of the PDPA. The PDPC has the power to issue advisory guidelines, which provide an indication as to how the PDPC will interpret the PDPA. However, the advisory guidelines are not legally binding and do not limit or restrict the PDPC’s administration and enforcement of the PDPA.

The PDPC published revised versions of: (1) the Advisory Guidelines on Key Concepts in the PDPA ("Key Concepts Guidelines") on 8 May 2015 and (2) the Advisory Guidelines on the PDPA on Selected Topics ("Selected Topics Guidelines") on 11 September 2014. The recent amendments to the Key Concepts Guidelines elaborate and provide examples in relation to the
PDPR and clarity on the consent obligation, the recent amendments to the Selected Topics Guidelines provide additional information on data activities relating to minors and a new chapter on photography.

On 8 May 2015, the PDPC published the Advisory Guidelines on Requiring Consent for Marketing Purposes, which provide guidance on whether organisations must obtain consent for the sending of marketing materials to individuals and using the individual’s personal data for other marketing activities. On 8 May 2015, the PDPC also published the Guide to Securing Personal Data in Electronic Medium, which provides information and examples on good practices which organisations may adopt to further secure electronic personal data and the Guide to Managing Data Breaches, which provides information which organisations may consider when formulating their framework for managing and minimising data breaches.

The PDPC has also recently issued the Sector Specific Advisory Guidelines for the Telecommunications, Real Estate Agency, Education, Healthcare and Social Service Sectors (“Sector Specific Guidelines”).

**Implementation of DNC Registry**

Organizations must check the DNC registry before sending marketing messages to consumers through their Singapore telephone numbers.

The PDPA prohibits organizations from sending marketing messages to telephone numbers listed on the relevant register (there are three: No Voice Call, No Text Message and No Fax Message), unless they have obtained “clear and unambiguous” consent from the relevant individual. Such consent should also be evidenced in writing or such other form suitable for subsequent reference, and should not be imposed as a condition for the provisions of goods or services. In practice, this is typically achieved by providing customers with a check box for customers to opt in to receiving marketing messages on their telephone numbers on a voluntary basis.

 Organizations can set up an account at [www.dnc.gov.sg](http://www.dnc.gov.sg) and begin purchasing credits to be used in conducting checks on the registry in preparation for the effective date.

The PDPC has issued an exemption allowing organizations with an on-going relationship with an individual to send marketing messages related to the subject of the on-going relationship to the individual via text or fax (but not voice calls), subject to the satisfaction of certain conditions, including the inclusion of a facility to allow the individual to opt out of receiving further marketing messages under the exemption.
2. Emerging Privacy Issues and Trends

*Data security breaches*

While there is no mandatory requirement around security breach notification under the PDPA, we anticipate that the PDPC may take action against organizations that are found to have taken inadequate security measures to protect Personal Data in their possession or under their control from unauthorized disclosure, particularly given the recent uptick in cybersecurity attacks. For example, the PDPC is currently investigating two cases of data security breaches - a potential loophole on the website of a major telecommunication operator and the hacking of a company’s membership database leading to the leak of personal details of its customers.

*Interface between the PDPA and social media*

It might be said that there is an inherent tension between data protection and interactions on social network platforms, which rely on the sharing of information, including Personal Data, to engage users. While the PDPA contains a number of broad exemptions that may be applicable in this context, including exemptions for the collection, use and disclosure of publicly available personal data, we foresee that data protection issues may nevertheless arise. For example, it is questionable whether a professional blogger who has been subjected to insulting or derogatory remarks on social media could collect and post personal information regarding the individuals who made such wanton postings on her blog without contravening the PDPA.

There was also a recent case in which the operator of an online forum was forced to disclose the identity of an individual who had allegedly made defamatory remarks under a pseudonym. In the absence of clear safeguards in the relevant terms of use, it may not be clear how the operator of a social networking platform should react if such a request were filed directly with the operator, particularly if the transgression complained of does not amount to an offense or if the offense is committed overseas.

*Do Not Call Registry*

Since the Do Not Call Registry rules came into force in January 2014, there have been two reported decisions. In the first case, a home tuition agency and its director were fined S$39,000 each for sending marketing messages to telephone numbers registered with the DNC Registry. In the second case, a property agent has been charged with 27 counts of contravention of the obligation to check the DNC Registry before sending telemarketing messages to Singapore telephone numbers.
**Data Protection Enforcement**

The PDPC is currently investigating a number of alleged breaches of the PDPA by organizations in Singapore. Apart from the data security breaches mentioned above, the PDPC is looking into a complaint that a company has breached the PDPA by disclosing a user’s Personal Data without his consent when he used his phone in Singapore and as a result he received unsolicited calls from overseas numbers.

### 3. Law Applicable

Prior to the introduction of the PDPA, Singapore’s approach towards data protection was sectoral in nature. In the private sector, only organizations in certain industries (e.g., banking and medical) were subject to some form of mandatory regulation. Even then, the regulation was generally limited to more sensitive data, such as information on bank accounts and health records.

The PDPA does not have any impact on mandatory requirements imposed under sectoral regulations. Organizations subject to such sectoral regulations are expected to comply with the baseline requirements set out in the PDPA, as well as additional requirements under such sectoral regulations.

The PDPA does not affect the rights of organizations to collect, use or disclose personal data to the extent that such collection, use or disclosure is authorized under other written laws.

### 4. Key Privacy Concepts

#### a. Personal Data

The definition of “Personal Data” in the PDPA would cover information, whether true or not, about an individual who can be identified from that piece of data or from that data and other data the organization has or is likely to have access to. Business contact information would generally fall outside the scope of the PDPA. Unlike the approach adopted in certain jurisdictions, limited protection is afforded to Personal Data of deceased individuals, in that obligations relating to the safeguarding and disclosure of such Personal Data would continue to apply for a period of 10 years.

The PDPA definition also covers all forms of Personal Data, whether electronic or non-electronic.

It is recognized that in line with the pro-consumer definition of Personal Data, it is not feasible for the PDPA to prescribe a definitive list of personal information that should be protected. The scope of the definition would depend on the context, as well as technological developments which may bring about new forms of Personal Data that is not currently envisaged.
b. Data Processing
The data protection rules in the PDPA apply to the collection, use and disclosure of Personal Data.

c. Processing by Data Controllers
Under the PDPA, a data intermediary processing personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing would have limited obligations in respect of the Personal Data. The data intermediary is only required to take reasonable security measures to safeguard the Personal Data and to delete or anonymise the Personal Data when it is no longer required for legal or business purposes. An organization, on the other hand, would be held responsible for the processing of Personal Data in its custody or under its control. In other words, Personal Data that is in the custody of the data intermediary, but under the organization's control, would nevertheless be covered.

All private sector “organizations” in Singapore would fall within the ambit of the PDPA. This would cover natural persons, trusts and other entities, corporate or unincorporated. However, acts of a natural person acting in a personal or domestic capacity are excluded.

More importantly, the PDPA would not apply to public agencies in Singapore.

d. Jurisdiction/Territoriality
There is no specific restriction of the application to the PDPA only to Personal Data or organisations in Singapore. An “organization” is defined as including any individual, company, association, or body of persons, corporate or unincorporated, whether or not (a) formed or recognized under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore. In general, every organization (unless exempted or excluded) is required to comply with the PDPA in respect of activities relating to the collection, use and disclosure of Personal Data in Singapore. Hence, the PDPA arguably has extraterritorial effect and foreign companies which engage in data collection activities in Singapore would still be required to comply with the PDPA.

e. Sensitive Personal Data
The PDPA is intended to establish the minimum or baseline standards applicable to the processing of Personal Data by private sector organizations, and will be supplemented by other legislative and regulatory regimes, such as the existing sectoral requirements mentioned in Section 3 above.

That being the case, the PDPA does not provide for a separate regime governing sensitive Personal Data. If more stringent requirements are required to be imposed in respect to the processing of such sensitive Personal Data, such concerns are likely to be addressed in sector-specific laws that apply concurrently.
f. Employee Personal Data

The PDPA covers Personal Data collected from employees of the organization. The rules which apply to the collection of such employee Personal Data may be slightly different (see Section 5(d) below).

5. Consent

a. General

The regime prescribed by the PDPA is based on consent, purpose and reasonableness. An organization would only be allowed to collect, use or disclose Personal Data with consent from the individual concerned. The consent obtained may be express or implied, depending on the circumstances. For example, if an individual voluntarily provides his Personal Data to a clinic when registering or making an appointment for medical treatment, he may be deemed to have given consent to the collection and use of such Personal Data by the clinic for that purpose.

The organization is also required to ensure that the collection, use or disclosure of Personal Data is for a reasonable purpose which the organization has disclosed to the individual before the collection of the Personal Data. The reasonableness of the purpose would be measured against what a reasonable person would consider appropriate in the circumstances.

The organization may not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of Personal Data beyond what is necessary to provide that product or service. Consent obtained through deception or by providing misleading or incomplete information would not be deemed to be validly given.

The individual should be allowed to withdraw his consent at any time. Where the organization receives notice from the individual pertaining to the withdrawal of consent, the organization may inform the individual of the likely consequences of such withdrawal, but cannot prohibit such withdrawal.

b. Sensitive Data

The PDPA is intended to prescribe the baseline requirements for the processing of Personal Data by private sector organizations and does not recognise a special category of Personal Data as sensitive Personal Data.

c. Minors

The PDPC has clarified in its Selected Topics Guidelines that it shall adopt the “rule of thumb” that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent to the collection, use and/or disclosure of his Personal Data by an organization on his own behalf. However, if an organization has reason to believe that the minor would not, the organization should obtain consent from the minor’s parent or guardian.
Similarly, consent may be obtained from a guardian or trustee appointed for the individual, an attorney appointed under a power of attorney, or any person with written authorisation from the individual to act on his or her behalf.

d. Employee Consent

The PDPA provides for certain exemptions that apply to the collection, use and disclosure of Personal Data of employees. There is a general exemption in respect of the reasonable collection, use and disclosure of Personal Data by an employer for the purposes of managing or terminating an employment relationship between the organization and an employee.

In order to be able to rely on this exemption, the organization needs to notify the employee that it is collecting Personal Data for such purposes and provide the contact information of an officer who can answer queries regarding the organization’s data protection policies upon request, but is not required to seek consent from the employees.

e. Online/Electronic Consent

The PDPA does not specifically address the issue of online/electronic consent, although The Key Concepts Guidelines and the PDPC’s publication “A Guide to Notification” provide some examples where consent may be obtained online or electronically.

Further, we note that it is likely that any consent provided online or electronically would be considered validly given under the Electronic Transactions Act.

6. Notice Requirements

An organization that collects personal data must provide data subjects with information about the organization’s identity, the types of personal data being collected, the purposes for collecting personal data, its privacy practices (which must be given in a clear and transparent way), third parties to which the organization will disclose the personal data, how to contact the privacy officer or the person accountable for the organization’s policies and practices, how to make an inquiry or file a complaint, and how to access and/or correct the data subject’s personal data.

7. Processing Rules

An organization that processes personal data must limit the use of the personal data to only those activities which are necessary to fulfill the identified purpose(s) for which the personal data was collected, and delete/ anonymize personal information once the stated purposes have been fulfilled and legal obligations met.
8. Rights of Individuals

The PDPA provides Data subjects the general right to be informed by an organization of the personal data the organization holds about the data subject and to access and correct Personal Data held by organizations.

Organizations are allowed to charge a reasonable fee to defray any costs that they would incur in allowing individuals to have such rights of access and correction.

9. Registration/Notification Requirements

The PDPC undertakes education and awareness efforts and is responsible for the enforcement of the PDPA. However, in order to keep compliance costs down for organizations, particularly small and medium-sized enterprises, the PDPC has adopted a complaint-based approach in exercising its oversight duties, and will only investigate cases of non-compliance where a complaint is filed. Organizations will not be required to submit reports to, or be audited by, the PDPC on a regular basis.

In keeping with the foregoing, the PDPA does not impose any mandatory requirements relating to registration with or notification to the PDPC.

10. Data Protection Officers

Under the PDPA, organizations are required to designate one or more employees to be responsible for ensuring their compliance with the law. Notwithstanding the fact that the designated employee(s) would be accountable for the organization’s compliance with the PDPA, designation of such employee(s) does not relieve the organization of its statutory obligations.

The business contact information of the designated employee(s) should be made known to individuals from whom Personal Data is collected, and to consumers generally. Such designated employee(s) should be able to address queries regarding the organization’s data policies on the collection, use and disclosure of Personal Data and the organization’s compliance with the law.

11. International Data Transfers

The PDPA provides that an organization should not transfer Personal Data outside of Singapore unless it complies with requirements prescribed under the Act to ensure that Personal Data would be afforded a comparable standard of protection. Under the PDPR, a transferring organization is required to take appropriate steps to ascertain whether, and to ensure that, the recipient of the Personal Data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations to provide to the transferred Personal Data a standard of protection that is at least comparable to the protection under the PDPA.
12. Security Requirements
Organizations are required to take steps to ensure that personal data in its possession and control are protected from unauthorized access and use, implement appropriate physical, technical and organization security safeguards to protect personal data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the personal data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. The organization may be liable together with the third party provider in case of breach by the latter.

14. Enforcement and Sanctions
Failure to comply with the PDPA can result in complaints and investigations/audits by the PDPC. The PDPC has broad powers to give directions to the infringing organization, including to order the payment of a financial penalty of up to S$1 million. Individuals who suffer loss or damage as a result of contravention of the data protection obligations in the PDPA have private rights of action and can commence civil proceedings against the organization. A contravention of the DNC provision in the PDPA is criminal in nature and may lead to the imposition of fines up to S$10,000 per offense.

15. Data Security Breach
While organizations that are involved in a data breach situation are not required by the PDPA to report the breach, such organizations shall assist authorities with any investigation relating to the breach, and comply with data authority orders and court orders.

16. Accountability
There is currently no requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of personal data.

17. Whistle-blower hotline
Whistle-blower hotlines may be established in Singapore provided that they are in compliance with local laws.

18. E-discovery
When implementing an e-discovery system, an organization may potentially be required to obtain the consent of employees if the collection of Personal Data is involved. However, it may be possible for the organization to argue that the implementation of the e-discovery system falls within the scope of the
employment exemption mentioned in Section 5(d) above, in which case specific consent is not required although the organization should notify the employees regarding the implementation of the system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

Similarly, when implementing an anti-spam filter solution into its operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace in order to rely on the employment exemption mentioned in Section 5(d) above.

20. Cookies

The Selected Topics Guidelines has clarified that the PDPA applies to the collection, use or disclosure of Personal Data using cookies. In particular, consent is generally required for cookies which collect Personal Data. However, for Internet activities that the user has clearly requested, there may not be a need to seek consent for the use of cookies to collect, use and disclose personal data where the individual is aware of the purposes for such collection, use and disclosure and voluntarily provided his Personal Data for such purposes.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a data subject (e.g., direct marketing is made to a Singapore telephone number subject to the Do Not Call requirements discussed in Section 1) is required to obtain the data subject’s prior express (opt-in) consent, which cannot be inferred from a data subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent may not be considered clear and unambiguous consent.
South Africa

Darryl Bernstein
Johannesburg
Tel: +27 (0) 11 911 4367
darryl.bernstein@bakermckenzie.com

Widaad Ebrahim
Johannesburg
Tel: +27 (0) 11 911 4384
widaad.ebrahim@bakermckenzie.com

Deepa Ramjee
Johannesburg
Tel: +27 (0) 11 911 4368
depa.ramjee@bakermckenzie.com
1. Recent Privacy Developments

Enactment of Data Protection and Privacy Legislation

While South African law recognises a general right to privacy in relation to a person’s information, there is currently nothing in South African law which expressly regulates the processing of personal information. On 26 November 2013, the new Protection of Personal Information Act, 2013 (the “Act”) was enacted. Only certain sections of the Act have commenced, namely Section 1 of Part A of Chapter 5 and Sections 112 and 113. These sections are specific to the establishment of the Information Regulator and his authority to draft and put forward regulations under the Act.

The Act seeks to bring South Africa in line with international data protection laws by regulating the processing of the information of natural and juristic persons and placing more onerous obligations on “responsible parties” that process such information. The Act sets out the essential parameters for the lawful processing of personal information, including:

- eight “core-information-protection principles”;
- a number of substantive issues concerning, inter alia, the processing, collecting, transferring and maintaining of personal information;
- exemptions from the information-protection principles;
- the rights of Data Subjects regarding unsolicited electronic communications and automated decision making;
- the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of the Act and the Promotion of Access to Information Act, 2000;
- the regulation of trans-border information flows; and
- enforcement mechanisms.

The Act introduces terminology and concepts which are, to a certain extent, novel to South African law, the broad formulation of which are likely to have significant implications in respect of both the citizens of South Africa whose information is processed by companies and public bodies, and the companies and public bodies doing the actual processing (whether this be in South Africa or not).

The Act will not apply to the processing of information:

- in the course of a purely personal or household activity;
- that has been “de-identified” (i.e., deleted to the extent that it cannot be retrieved);
by or on behalf of the State, relating to national security, investigation of offences, and the like;

• for exclusively journalistic purposes by responsible parties who are subject to a code of conduct by virtue of office;

• by cabinet, provincial executive councils and municipal councils; and

• relating to the judicial conduct of a court.

We note the following salient principles arising from the Act:

• Personal information may only be processed in a fair and lawful manner that is transparent to the individual, and requires an individual’s explicit consent.

• Responsible parties processing information must ensure that personal information is only processed for specific, explicitly defined and legitimate reasons relating to the functions or activities of the organization, and the organization must take steps to make affected Data Subjects aware of the purposes for which the personal information will be processed. Personal information may only be kept for as long as it is required to fulfil the purpose for which it was collected.

• A responsible party is required to:
  o appoint an Information Officer and Deputy Information Officer to ensure compliance with the conditions set out in the Act and deal with complaints from Data Subjects who seek to enforce the Act;
  o maintain documentation of all processing; and
  o secure the integrity and confidentiality of personal information in its possession or under its control and ensure that it is appropriately safeguarded against loss, destruction or unlawful access.

2. Emerging Privacy Issues and Trends

a. The Act

The enactment of the Act itself, largely based on similar US and UK data protection legislation, is the most significant development in the South African privacy landscape. It is expected that the Act will come into force during the last six months of 2015. The timeline for the commencement of the entire Act is, however, still unclear. Once fully operative, responsible parties will have one year to ensure legal compliance.

Given the limited transitional period provided for compliance coupled with potentially severe penalties, clients have already commenced with the implementation of initiatives in an effort to comply with the prescriptive principles under the Act. The focus of many compliance programs have been
on the overlap between the Act and other laws, since a law which gives the Data Subject greater protection will prevail over the Act. Implementation of the Act and the enforcement issues which will no doubt flow from it will continue to be a hot topic moving forward.

b. Electronic Signatures

In South Africa our Supreme Court of Appeal has recently handed down an award in relation to amendments to an agreement which are required to be in writing and signed by the parties. An agreement, which provided for consensual cancellation to be recorded in writing and signed by the parties to be valid, was terminated by an exchange of e-mails. Although not physically reduced to pen and paper, the court was prepared to uphold the cancellation.

3. Law Applicable

The Constitution of the Republic of South Africa, 1996 (the “Constitution”) recognises a general right to privacy. Data protection and privacy issues are also currently regulated under the common law and various sector specific statutes and laws, governing particular aspects of data protection.

Under the common law, privacy embraces all those personal facts which the person concerned has determined to exclude from the knowledge of outsiders and intends to keep private. The Constitution provides, in Section 14, that everyone has the right to privacy, which includes, on a broad interpretation, the right:

- to protection against the unlawful collection, retention, dissemination and use of personal information; and/or
- not to have the privacy of their communications infringed.

The Constitutional right of privacy is not absolute and an infringement of the right may be justifiable in terms of the general limitation clause in the Constitution. What constitutes a reasonable and justifiable limitation will depend on the circumstances of each case. A high level of protection is given to the intimate personal sphere of life, and a lower level is given to the business, commercial and public spheres of life.

Generally, ordinary delictual (tort) remedies such as a claim for personal injury, patrimonial loss and/or an injunctive relief would be available for a claim arising from wrongful data processing.

The Electronic Communications and Transactions Act, 1998 (“ECT Act”) prescribes certain principles for the electronic collection of personal information of individuals. Under the ECT Act, a data controller (being a person who electronically requests, collects, collates, processes or stores personal information from or in respect of any natural person) would only be required to subscribe to the data protection principles if it has voluntarily agreed to do so with the Data Subject.
The stated purpose of the Act is to give effect to the constitutional right to privacy. The Constitution, together with the Act, will regulate the parameters for the lawful processing and protection of personal information by automated and manual means.

4. Key Privacy Concepts

a. Personal Data
The Act applies to the processing of personal information of natural and juristic persons. “Personal information” is defined as information relating to identifiable, living natural and juristic persons, including:

- information relating to demographics such as the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, or contact details such as the e-mail address, physical address, telephone number or other particular assignment to the person;
- the blood type or any other biometric information of the person;
- the personal opinions, views or preferences of the person or the views or opinions of another individual about the person;
- correspondence sent by the person that is of a private or confidential nature; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

The Act applies to the exclusion of any provision of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object, or a specific provision, of the Act. If any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in Act, the extensive conditions prevail.

b. Data Processing
The Act applies to manual and automated data processing. “Processing” is broadly defined as activity, whether automated or not, concerning personal information, which includes:

- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
• dissemination by means of transmission, distribution or making available in any other form; or
• merging, linking, blocking, degradation, erasure or destruction of information.

Personal information may only be processed if:
• the Data Subject or a competent person, where the Data Subject is a child, consents to the processing;
• processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party;
• processing complies with an obligation imposed by law on the responsible party;
• processing protects a legitimate interest of the Data Subject;
• processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

c. Processing by Data Controllers
The Act applies to those responsible parties who determine the purposes for which and the manner in which any Personal Information is, or is to be, processed. A responsible party is defined in the Act as a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

d. Jurisdiction/Territoriality
The provisions of the Act will apply to the processing of personal information entered in a record by or for a responsible party that is domiciled in South Africa. The Act will also apply where the responsible party is not domiciled in South Africa but is using either automated or non-automated means to process personal information in South Africa.

e. Sensitive Personal Data
Subject to specific limitations and additional requirements, the Act expressly prohibits the processing of “special personal information” -- that is, personal information relating to:
• the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a Data Subject; or
• the criminal behaviour of a Data Subject to the extent that such information relates to:
  o the alleged commission by a Data Subject of any offence; or
any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.

The prohibition on processing special personal information does not apply if the:

- processing is carried out with the consent of a Data Subject;
- processing is necessary for the establishment, exercise or defence of a right or obligation in law;
- processing is necessary to comply with an obligation of international public law;
- processing is for historical, statistical or research purposes to the extent that:
  - the purpose serves a public interest and the processing is necessary for the purpose concerned; or
  - it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the Data Subject to a disproportionate extent;
- information has deliberately been made public by the Data Subject; or
- provisions of specific sections in the Act relating to the relevant types of special personal information, are complied with.

The Information Regulator may, subject to subsection 27(3), upon application by a responsible party and by notice in the Government Gazette, authorise a responsible party to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the Data Subject. The Regulator may impose reasonable conditions in respect of any such authorization.

f. Employee Personal Data

South African employment legislation requires every employer to keep a record of certain basic information on an employee, including:

- The employee’s name and occupation;
- the time worked by each employee;
- the remuneration paid to each employee;
- the date of birth of any employee under 18 years of age; and
- any other prescribed information.
A record must be kept by the employer for a period of three years from the date of the last entry in the record. The collection of such information from the employee may be collected without employee consent, as it is required by law, and an employer will generally be able to justify processing such information.

The restrictions on processing special personal information about an employee are however more stringent and would need to comply with local employment legislation and the Act. For example, the record of any medical examination performed in terms of the Basic Conditions of Employment Act, 1997 must be kept confidential and may be made available only:

- in accordance with the ethics of medical practice;
- if required by law or court order; or
- if the employee has, in writing, consented to the release of that information.

5. Consent

a. General

Consent of the Data Subject, though not mandatory, is listed as a justification for processing of personal information under the Act. The Act defines “consent” as any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information. Under the Act and prior to the collection of the information, or as soon as possible thereafter, the responsible party must take reasonable steps to ensure that the Data Subject is aware of:

- the information being collected and where the information is collected from the Data Subject, the source from which it is collected; the name and address of the responsible party;
- the purpose for which the information is being collected; whether or not the supply of the information by that Data Subject is voluntary or mandatory; the consequences of failure to provide the information; any particular law authorising or requiring the collection of the information; the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation; any further information such as the: recipient or category of recipient of the information; nature or category of the information;
- the existence of his or her right of access to and the right to rectify the information collected; the existence of the right to object to the processing of personal information; and the existence of the right to lodge a complaint with the Information Regulator and the contact details of the Information Regulator, which are necessary, having regard to the specific
circumstances in which the information is or is not to be processed to enable reasonable processing.

The form of consent has not been prescribed; however, it is likely that in order to demonstrate consent for purposes of the Act, the responsible party will need to prove compliance with the above requirements.

b. Sensitive Data

The processing of information relating to the race and ethnic origin of a Data Subject, for diversity monitoring purposes would, under relevant employment equity legislation, require the written consent of the employee, in the prescribed form. In addition the collection of any health-related information requires the written “informed” consent of the patient.

The Act expressly prohibits the processing of special personal information. This prohibition on processing special personal information under the Act does not apply however if the processing is carried out with the consent of a Data Subject. The form of consent, though not prescribed under the Act, should be explicit and clear and should include reference to the requirements listed in paragraph 5a above.

c. Minors

The Act provides that a responsible party may not process personal information concerning a child (being a natural person under the age of 18 years). However, the prohibition on processing personal information of children does not apply if:

- the processing is carried out with the prior consent of a competent person (being any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child);
- necessary for the establishment, exercise or defence of a right or obligation in law;
- necessary to comply with an obligation of international public law;
- for historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned;
- or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- personal information which has deliberately been made public by the child with the consent of a competent person.
The Information Regulator may, upon application by a responsible party and by notice in the Government Gazette, authorise a responsible party to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child. The Regulator may impose reasonable conditions in respect of any authorization so granted.

d. Employee Consent
There is no provision under the Act that specifically addresses consent requirements for employees. With reference to paragraph (4.f) above, it is noted that depending on the type of information collected, local employment legislation may require that consent be procured in writing.

e. Online/Electronic Consent
Electronic consent is permissible and can be effective in South Africa provided that it is properly structured and evidenced.

6. Information/Notice Requirements
Under the Act, an organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to contact the privacy officer or other person accountable for the organization’s policies and practices; how to make an inquiry or complaint; how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

7. Processing Rules
Under the Act, an organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected.

8. Rights of Individuals
Under the Act, Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data.
9. Registration/Notification Requirements
Under the Act, organizations that collect and process Personal Data may be required to file with and notify the appropriate data authority.

10. Data Protection Officers
Under the Act, organizations are required to register a privacy officer or other individual who will be accountable for the privacy practices of the organization with the data protection authority to be established.

11. International Data Transfers
Currently, there is nothing in South African law that expressly restricts/limits the international transfer of personal information. Under the Act however, a responsible party in South Africa may not transfer personal information about a Data Subject to a third party located in a foreign country unless:

- the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection that effectively upholds the principles for reasonable processing of information which are substantively similar to the principles applicable in South Africa;
- the law, binding corporate rules or binding agreement includes provisions that are substantially similar to those in the section of the Act relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
- the Data Subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and the responsible party; or
- the transfer is for the benefit of the Data Subject and it is not reasonably practicable to obtain the consent of the Data Subject to that transfer; and
  if it were reasonably practicable to obtain such consent, the Data Subject would be likely to give it.

For clarification, it is noted that within the context of the above:

- “binding corporate rules” means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country; and
- “group of undertakings” means a controlling undertaking and its controlled undertakings.
12. Security Requirements

Under the Act, organizations are required to take steps to: ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organizational security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties may be required to use contractual or other means to protect Personal Data, and may be required to comply with sector specific requirements. Under the Act, organizations shall be held liable together with third party providers in case of breach by the latter.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings, and/or private rights of action.

15. Data Security Breach

The Act provides for the notification of security compromises. Where there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Regulator and the Data Subject, unless the identity of such Data Subject cannot be established.

The notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party’s information system.

The responsible party may only delay notification of the Data Subject if a public body responsible for the prevention, detection or investigation of offences or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned.

The notification to a Data Subject must be in writing and communicated to the Data Subject in at least one of the following ways:

- emailed to the Data Subject’s last known physical or postal address;
- sent by e-mail to the Data Subject’s last known e-mail address;
• placed in a prominent position on the website of the responsible party;
• published in the news media; or
• as may be directed by the Regulator.

The notification must provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including:

• a description of the possible consequences of the security compromise;
• a description of the measures that the responsible party intends to take or has taken to address the security compromise;
• a recommendation with regard to the measures to be taken by the Data Subject to mitigate the possible adverse effects of the security compromise; and
• if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

The Information Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a Data Subject who may be affected by the compromise.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions and/or class actions.

16. Accountability

Under the Act, organizations are required to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in South Africa provided that they are in compliance with local laws.

18. E-Discovery

When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of Personal Data is involved, and advise the employees of the implementation of such system, the monitoring of work tools and the storage of information.
19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace. They may be required to give employees the opportunity to opt-out from the spam-filtering solution, and give the employees the opportunity to review the isolated emails designated as spam.

20. Cookies

The use of cookies must comply with data privacy laws. As such, consent of Data Subjects may have to be obtained before cookies can be used and deployed.

Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

Under the Act, an organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. Consent of the Data Subject must be obtained for a specific activity. Bundled consent is not considered valid consent.

Currently, responsible parties are required to afford a recipient of direct marketing communications the opportunity to opt-out at no cost.
South Korea

Boseong Kim
Seoul
Tel: +82 2 721 4130
boskim@kcllaw.com

Junghwa Lee
Seoul
Tel: +82 2 721 4147
jhlee@kcllaw.com

Mike Shin
Seoul
Tel: +82 2 721 4140
mikeshin@kcllaw.com
1. Recent Privacy Developments

Amendments to the Act on Promotion of Information and Communications Network Utilization Act

- **Strengthening remedy for security breach**

The key intention of the amendments to the Act on Promotion of Information and Communications Network Utilization (the “Amended Act”) is to strengthen remedy for security breach. A legal damages system is newly introduced by the Amended Act, under which aggrieved individuals due to security breaches may receive compensation of up to KRW 3 million without proving their damages (the relevant telecommunication service provider would not be held liable if it proves that there is no intentional act or negligence on its part).

- **Strengthening corporate obligations and the level of sanctions for violations**

The Amended Act strengthens sanctions for violations of personal information protection related provisions by companies. Under the Amended Act, the applicable penalty is equal to the relevant revenues multiplied by the rate of 3% or lower, while it was equal to the relevant revenues multiplied by the rate of 1% or lower under the previous Act. In addition, for the event of a security breach, the previous Act provided for the fixed amount of penalty (of up to KRW 100 million), but the Amended Act provides for the fixed rate of penalty, which is up to 3% of the relevant revenues.

- **Strengthening the regulation on spam**

Under the Amended Act, a person may transmit marketing messages via e-mail for commercial purposes after having obtained the express prior consent of the recipients, while under the previous Act, a person is prohibited from transmitting marketing messages via e-mail only when the recipient has opted out of receiving them.

**Amendments to the Personal Information Protection Act**

- **Limiting the collection, use and processing of resident registration numbers**

Under the Amended Personal Information Protection Act (the “Amended PIPA”), public organizations and private business operators are prevented from unnecessarily collect resident registration numbers without grounds based on the applicable laws.
• **Introducing a new event for penalty**

The penalty provision is newly introduced by the Amended PIPA, under which if an entity fails to take measures to ensure security and there occurs a security breach that results in a leak of resident registration numbers, the entity may be subject to a penalty of up to KRW 5 million.

• **Judicial precedent on security breach**

Korean courts used to relatively be reluctant to recognize a fault on the part of companies in connection with their security breaches, but recently there is a change in such position of Korean courts. For a claim for damages resulting from a security breach filed against KT Corporation (telecom company), the Seoul Central District Court has ruled that KT Corporation shall pay KRW 2.87 billion to the plaintiffs in the aggregate (which is KRW 100,000 for one plaintiff), finding that KT was negligent in managing the IDs, passwords and user accounts in its intranet and that it is highly likely that leaked personal information is accessed by others and there is a possibility of additional duplication and subsequent leakage. As KT Corporation appealed this decision, the case is now litigated in an appellate court.

2. Emerging Privacy Issues and Trends

**Big data processing companies** - There have been discussions about how to regulate big data processing companies in their use of personal information. The Korea Communications Commission is in the process of preparing relevant guidelines.

**Strengthening the regulation on personal information processing and crackdown on violations** – In an effort to reduce damages resulting from security breaches, the relevant regulations are strengthened (e.g., restriction on collecting resident registration numbers), and regulatory authorities are strengthening their crackdown on personal information infringers.

**Social Media** - In theory, the regulations concerning social media are applicable to both domestic and foreign entities, but, in practice it is difficult to enforce them against foreign entities (e.g., Facebook, Twitter, etc.), which raises a concern about appropriate protection of users. Commentators are having on-going discussions about that.

**Privacy breach** – As security breaches in companies have continued to occur, sanctions for such events are being strengthened. In addition, recently we have seen cases in which a privacy breach incident developed into a class action.

**Employee Monitoring** - Commentators began a discussion about this several years ago, but it has been relatively inactive partly due to other more pressing labor and management issues.
Illegal sale of personal information - The illegal sale of personal information of customers has become an issue, and commentators are discussing the ways to regulate such illegal sale.

Other than the above, we see an increasing discussion concerning personal information protection issues associated with the development of technology for the “Internet of Things” and the “right to be forgotten.”

3. Law Applicable

The applicable privacy/information laws are as follows:

The general law governing the protection of personal information is (i) the Personal Information Protection Act, the information and communications service providers are regulated by (ii) the Act on Promotion of Information and Communications Network Utilization and Information Protection, and personal credit information handled by financial institutions is governed by (iii) the Act on Use and Protection of Credit Information.

Below are the hyperlinks to the applicable laws in the Korean language:

(i) Personal Information Protection Act (“PIPA”)

   Enforcement Decree of the PIPA
   Enforcement Rules of the PIPA

(ii) Act on Promotion of Information and Communications Network Utilization and Information Protection (“Information and Communications Network Act”)

   Enforcement Decree of the Information and Communications Network Act
   Enforcement Rule of the Information and Communications Network Act

(iii) Act on Use and Protection of Credit Information (“Credit Information Act”)

   Enforcement Decree of the Credit Information Act
   Enforcement Decree of the Credit Information Act

The website operated by the Korea Legislation Research Institute (http://elaw.klri.re.kr/eng_service/main.do) provides English translations of some laws, and you can have access to them after becoming a member (which is free of charge). However, some of the laws are not up to date, and we cannot guarantee the accuracy of such translations.
4. Key Privacy Concepts

a. Personal Data

Under the PDPA, “personal data” means data pertaining to a living person, including their name, resident registration number, images, etc., by which the individual can be identified. The PDPA provides no specific requirements in terms of the types, forms and characteristics of the data, or on data processing methods or media in determining whether certain information constitutes personal data.

Under the Information and Communications Network Act, “personal data” means data in the form of code, letter, voice, sound, image, etc., that pertains to a living individual and identifies a specific person through the name, resident registration number, etc.

The definition of personal data under the PDPA is broader than that under the Information and Communications Network Act. Other area-specific laws that cover privacy-related issues impose requirements on other limited types of personal data.

b. Data Processing

Under the PDPA, processing is comprehensively defined to mean collecting, creating, recording, saving, retaining, processing, editing, searching, printing out, correcting, restoring, using, providing, disclosing, destroying personal data, and other similar acts.

c. Processing by Data Controllers

Under the PDPA, a “personal data processor” means a public institution, corporate body, organization, individual, etc. that processes personal data directly or via another person to administer personal data files as part of their duties. Personal data files mean an aggregate of personal data systematically arranged or organized according to specific rules in order for the personal data to be readily retrievable.

Under the Information and Communications Network Act, data controllers are limited to those who provide information and communications services.

Under the Credit Information Act, data controllers are limited to those who provide or use credit information.

Korean privacy law regulates personal data processors but does not distinguish between data controllers and data processors. Therefore, the most likely interpretation of the law is that both data controllers and data processors are subject to the same obligations.
d. **Jurisdiction/Territoriality**

The application of Korean privacy law including the PDPA is not limited based on where the collection or processing of personal data occurs. Thus, in theory, companies located overseas that collect personal data of users in Korea are subject to Korean privacy law. In practice, however, it is very rare that Korean judicial authorities enforce Korean privacy law in such cases.

e. **Sensitive Personal Data**

The PDPA imposes additional requirements relating to the handling of (i) “sensitive data,” including ideas, belief, membership in or withdrawal from a labor union or political party, political views, health, etc., and genetic information and criminal records, and (ii) “unique identifying data,” including resident registration number, passport number, driver’s license number and alien registration number.

Processing of such sensitive data and unique identifying data is prohibited with only limited exceptions.

f. **Employee Personal Data**

Employee personal data was previously unregulated, but since the PDPA came into force, employee personal data should be treated in the same way as any other personal data.

As discussed in Section 5(d) below, an employer may collect and use personal data of an employee for the purposes of entering into and performing an employment contract. The PDPA does not, however, go on to address the permitted scope or limitations on an employers’ collection/use of employee personal data without the employee’s consent.

5. **Consent**

a. **General**

Under the PDPA, consent of the data subject is generally required prior to the collection, use or provision of personal data to third parties, subject to certain exceptions including: when it is required or permissible by law; necessary to perform an agreement with the data subject; or urgency of purpose to protect life, body or property.

Consent must be voluntary, informed, explicit and unambiguous. Consent can be provided by way of signature, clicking on a consent button (e.g., “I Agree” or “I Consent”) or by telephone, etc.

When obtaining the consent of a data subject, a personal data processor is required to set notify the data subject of the specific matters requiring consent so that the data subject can clearly understand what consent is being sought. Consent of the data subject only covers identified purposes. Fresh consent is required for purposes not previously identified and consented to.
The data subject can withdraw his consent at any time.

b. **Sensitive Data**

Sensitive data is recognized as a special category of personal data.

Under the PDPA, a personal data processor is required to obtain a data subject’s separate consent (i.e., in addition to the consent obtained for processing of general personal data) for the processing of sensitive data and for the processing of unique identifying data.

c. **Minors**

Consent cannot be obtained from minors, but can be given by a legal guardian or parent.

When a personal data processor obtains the consent of a legal representative of a child under the age of 14, the minimum information necessary for obtaining the consent of the legal representative (e.g., the name, contact information of the legal representative) may be collected from the relevant child without the consent of his or her legal representative.

d. **Employee Consent**

Since the collection/use of personal data is necessary for entering into and performing an employment contract with an employee, certain personal data of an employee may be collected/used without the employee’s consent. However, the Ministry of Public Administration and Security (“MOPAS”) has made it clear that employers should notify employees of all relevant matters concerning the collection/use of their personal data in their employment contract.

In addition, installation of employee surveillance equipment (e.g., CCTV, GPS) in a place of business is subject to discussions with the labor-management consultation council, but there are no provisions providing for penalties for breach of this requirement.

e. **Online/Electronic Consent**

Electronic consent is permissible and can be effective in South Korea if it is properly structured and evidenced.

The PDPA allows for consent to be obtained from the data subject through a process on the Internet (e.g., clicking on a consent button), electronic mails, electronic documents, mobile phone text messages, etc.

6. **Information/Notice Requirements**

An organization that collects personal data must provide data subjects with information about the organization’s identity; the types of personal data being collected; the purposes for collecting personal data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the personal data; the consequences of not
providing consent; the rights of the data subject; how the personal data is to be retained; where the personal data is to be transferred; how to contact the privacy officer or other person accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; how to access and/or correct the data subject’s personal data; and the duration of the proposed processing.

7. Processing Rules

An organization that processes personal data must limit the use of the personal data to only those activities which are necessary to fulfill the identified purpose(s) for which the personal data was collected; and delete/ anonymize personal data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data subjects have the general right to: be informed by an organization of the personal data the organization holds about the data subject and how the personal data is being processed; access the data subject’s personal data subject to some restrictions and/or qualifications; request the correction of the data subject’s personal data; request the deletion and/or destruction of the data subject’s personal data; and exercise the writ of habeas data.

9. Registration/Notification Requirements

There are no requirements for organizations that collect and process personal data to register, file or notify the local data authority.

10. Data Protection Officers

Organizations are required to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

The PDPA specifies the qualifications for a data protection officer, his duties and other related matters. The Information and Communication Network Act contains similar provisions. Depending on the size of the company, the owner or authorized representative of the company can act as the data protection officer in lieu of designating a separate data protection officer.

11. International Data Transfers

Organizations may transfer personal data outside of South Korea provided that reasonable steps have been taken to safeguard the personal data to be transferred.

The PDPA sets out procedures required to be followed by a personal data processor in order to transfer personal data to third parties in other jurisdictions. The Information and Communications Network Act also provides for the procedures for transfers of personal data to other jurisdictions and related protective measures.
12. Security Requirements
Organizations are required to take steps to ensure that personal data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect personal data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the personal data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose personal data to third parties are required to use contractual or other means to protect personal data, and may be required to comply with sector specific requirements. Organizations shall be liable together with third party providers in case of breach by the latter.

The PDPA provides for matters concerning the scope of outsourcing, disclosure of the outsourcer, the organization’s obligation to manage and supervise the outsourcer’s work, limitation on the scope of personal data processing by outsourcers, the organization’s liability for damages, etc.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, class actions, criminal proceedings, and/or private rights of action.

15. Data Security Breach
Under the PDPA, in the event of a data breach, the personal data processor must notify the data subject of such an event according to the prescribed methods of notification. In the event of large-scale security breaches, the PDPA imposes the requirement to notify the MOPAS or other specialized agencies and provides for follow-up measures.

The Information and Communications Network Act contains provisions dealing with incidents of security breaches of information and communications networks.

In addition, organizations that are involved in a data breach situation are required to: gather information about the breach; assess the potential risk of harm to the data subject; take steps to mitigate the harm to impacted data subjects; take steps to contain the breach and prevent future similar breaches; assist authorities with any investigation relating to the breach; and comply with data authority orders and court orders.
An organization that is involved in a data breach situation may be subject to suspension on the processing of personal data, an administrative fine, penalty or sanction, civil actions and/or class actions, or a criminal prosecution.

16. Accountability
Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of personal data.

17. Whistle-Blower Hotline
There are no laws/rules that regulate whistle-blower hotlines in South Korea.

18. E-Discovery
South Korea does not have a system equivalent to e-discovery under U.S. law. An organization, however, may be required to provide personal data pursuant to a court order.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace, and give employees the opportunity to review the isolated emails designated as spam.

20. Cookies
The use of cookies must comply with data privacy laws. Consent of data subjects may have to be obtained before the use and deployment of cookies.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a data subject is required to obtain the data subject’s prior consent, which may not be inferred from a data subject’s failure to respond.

Where consent is sought for marketing or soliciting the sale of goods or services as part of the sale of any goods or services, the personal data processor cannot refuse to provide such goods or services on the grounds that the data subject refused to consent to receive marketing or sales information.
Spain

Rosario Alvarez
Madrid
Tel: +34 91 230 4513
rosario.alvarez@bakermckenzie.com

Jordi Masdevall
Barcelona
Tel: +34 93 206 0820
jordi.masdevall@bakermckenzie.com

Maria Pons
Barcelona
Tel: +34 932551117
maria.pons@bakermckenzie.com

Raul Rubio
Madrid
Tel: +34 91 436 6639
raul.rubio@bakermckenzie.com
1. Recent Privacy Developments

Guidance on Privacy Impact Assessments

The Spanish Data Protection Authority (“SDPA”) issued a guide on privacy impact assessments (PIA) aimed at the promotion of a proactive privacy protection culture by providing guidance to companies in implementing PIAs as a necessary step in their internal processes.

Supreme Court decides on IP addresses

The Supreme Court (judgment dated 3 October 2014) concluded that IP addresses are personal data as they contain information concerning identified or identifiable individuals. The argument that there are no means to identify and associate the individual with an IP address was not accepted by the Supreme Court as it is possible to identify an individual with an IP address through third parties, e.g., Internet access services providers that know personal details of the individual who was provided with an IP address.

2. Emerging Privacy Issues and Trends

Employee monitoring - In a criminal case initiated by a company against an employee for fraud and forgery offences, the Criminal Chamber of the Spanish Supreme Court (judgment dated 16 June 2014), based on a literal interpretation of the fundamental right to the secrecy of communications, held that the interception of communications in the course of criminal proceedings requires a prior court authorization. Otherwise the interception is illegal and the evidence presented will not be admissible, no matter the equipment ownership (e.g., company’s computer), the communication channel (e.g., work email) or when and where the communication occurred (e.g., in the workplace during working hours). The traffic data and also the communications content once they are received and opened by the recipient (e.g., emails) are, however, excluded from the scope of the right to secrecy of communications.

3. Law Applicable

- The Spanish Data Protection Act No. 15/1999 (“SDPA”), which transposes the Data Protection Directive 95/46/EC into national law.

- The Royal Decree No. 1720/2007 (“Regulation”), which approves the regulation implementing the SDPA.

- Instruction No. 1/2006 of the Spanish DPA on the processing of Personal Data for surveillance purposes through camera systems.
4. Key Privacy Concepts

a. Personal Data
The SDPA applies to the processing of any alphanumeric, graphic, photographic, acoustic or any other type of information ("Personal Data" or "Data") relating to an identified or identifiable individual ("Data Subject").

b. Data Processing
"Processing" is broadly defined and covers any operation or technical process, whether automated or manual, performed on Personal Data that allows the collection, recording, storage, production, amendment, consultation, use, rectification, blocking and deletion, as well as the disclosure of Personal Data resulting from communications, consultations, interconnections and transfers. The SDPA and DPAR apply to both automated and manual data processing.

Notwithstanding the foregoing, the DPAR foresees the following exemptions to the application of Spanish data protection legislation:

- Contact details of individuals providing their services within legal entities would fall out of the scope of data protection regulations provided: (i) the categories of data processed relate only to first and last name, position, business address, email address, and phone and fax business numbers; and (ii) the purpose for processing such information shall be limited to the mere maintenance of the business relationship.

- Contact details of sole traders would fall out of the scope of data protection regulations provided: (i) the categories of data processed refer to the sole trader exclusively with regard to its trader, industrial or ship-owner conditions; and (ii) the purpose of processing such information is of a commercial nature, i.e., the Data Subject concerned with the Data processing activities is the private entity formed by the trader, industrial or ship-owner and not said persons themselves.

c. Processing by Data Controllers
The SDPA and DPAR apply to those entities that determine the purposes and the manner in which any Personal Data is to be processed ("Data Controller").

d. Jurisdiction/Territoriality
The SDPA and DPAR apply to:

- Data Controllers conducting their activities through an establishment in Spain. In this sense, where no Data Controller is established in Spain but data is processed by means of a Data Processor established in Spain, the Data Processor will be bound by the technical and organizational security measures set forth by Title VIII of the DPAR; or
the processing of Personal Data taking place outside of Spain but subject to Spanish law pursuant to international public law rules; or

Data Controllers that do not have any establishment in the EEA but that use any means located in Spain to carry out data processing activities other than merely for the purpose of transit (e.g., where Personal Data is collected by a Spanish affiliate or where a web site is located in Spain). In this case, the Data Controller must designate a representative established in Spain.

“Establishment” shall be considered, irrespective of its legal structure, as any stable installation allowing the effective and real undertaking of an activity.

e. Sensitive Personal Data

The SDPA imposes additional requirements for the processing of Sensitive Personal Data – that is, information relating to ideology, religion, beliefs, racial origin, health or sexual life, trade union membership, and criminal or administrative offenses. Data Subjects may not be compelled to disclose their ideology, beliefs or religion. Explicit and written consent to the processing of Personal Data relating to trade union membership, ideology, religion and beliefs must be obtained. Except as indicated below, the processing of Personal Data relating to health, racial origin and sexual life requires the prior express consent of the Data Subject, although it need not be given in writing. Data relating to criminal records and administrative sanctions may not be processed by a private Data Controller (even with consent of the Data Subject) except by duly authorized public institutions.

Specifically, the processing of Sensitive Personal Data is prohibited unless certain conditions are met, for example:

- the Data Controller obtains the explicit (and written) consent of the Data Subject (see Section 5(b) below);
- the processing is necessary to carry out the obligations and rights of the Data Controller in the field of employment, social security and health, and safety laws;
- the processing is necessary to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent;
- the processing is carried out in the course of legitimate activities with appropriate guarantees by political parties, trade unions, churches or other religious communities, foundations, associations or any other non-profit-seeking bodies only in respect of the relevant sensitive Personal Data (for example, political parties are exempted from consent only in respect of the processing of ideology information) and provided other conditions are met; or
• the processing is performed by a health care professional or institution under an obligation of secrecy, for the provision of medical advice or treatment.

f. Employee Personal Data

Employee Personal Data is likely to include sensitive Personal Data (e.g., health-related information) and non-sensitive Personal Data. Sensitive employee Personal Data may be processed in the circumstances mentioned in Section 4 (e) above and, in particular:

• where the Personal Data is health Data, the employer may process the start and end date of any sickness or absence (which is considered to be processing of Personal Data by the Spanish DPA) for compliance with social security requirements – that is, in order to comply with its obligations under employment, social security and health and safety laws as well as the grade of disability of the employee prior consent is not required. However, should the Data Controller wish to process any additional information (such as the reason for absence or medical certificates), the Data Controller would have to seek the prior express consent of the employee to the processing of such Personal Data and have a legitimate purpose for processing such data;

• where the Personal Data relates to the employee’s ability to perform “dangerous” or “very dangerous” activities or any activities which require a medical assessment for the prevention of “occupational risks” (as they are defined under the Spanish Labor Risks Prevention Act), this may be processed without prior consent. However, should the Data Controller be required to conduct a medical assessment of the ability of employees to perform activities, the Spanish Labor Risks Prevention Act provides that the Data Controller may process only a “fit for work/unfit for work” result without prior consent, and may not process a description of the specific health conditions of the employee. In addition, should the Data Controller wish to conduct any other type of medical assessment (e.g., physical exams, recruitment medical exams, etc.), it should generally obtain the prior express consent of the employee and have a legitimate purpose for processing such data; and

• where the Personal Data relates to trade union membership, this may be processed to the extent necessary to comply with legal and/or collective bargaining agreement obligations, provided that other specific requirements are met.

Non-sensitive employee Personal Data may be processed by a Data Controller in the circumstances mentioned in Section 5 below and, in particular, for the following purposes: human resources management, payroll, management of benefit plans (life and health insurances, stock option plans, etc.), training programs, legal requirements (social security and tax
withholdings), annual evaluations and when processing is necessary for the execution of an agreement to which the Data Subject is a party. A fallback justification for processing both sensitive and non-sensitive Personal Data in the employment context may be if consent is provided by the Data Subject.

In early 2010, the Spanish DPA issued a series of guidelines which aim to gather under a single document its existing opinions and recommendations concerning the processing of data within employment relationships so as to provide both private and public organizations with a tool to make compliance with the requirements set forth by Spanish data protection regulations easier. The guidelines are split into five chapters: (i) human resources; (ii) labor risk prevention; (iii) monitoring activities conducted by employers; (iv) relationship with trade-unions and (v) obligations of employees when accessing personal data related to them.

5. Consent

a. General

Consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data.

Consent of the Data Subject only covers identified purposes. Fresh consent is required for purposes not previously identified and consented to.

The Data Subject also has the right to withdraw consent at any time in given circumstances.

b. Sensitive Data

Explicit and written consent to the processing of data relating to trade union membership, ideology, religion, and beliefs must be obtained. The processing of data relating to health (except in compliance with labor, social security and health, and safety regulations), racial origin and sexual life requires the prior express consent of the Data Subject, although it need not be given in writing.

c. Minors

Under the DPAR, minors over 14 years of age may give valid consent to the processing of their Personal Data, to the extent that it is accepted that such minors have, in such cases, sufficient personal capacity of judgment to provide such consent. The consent of parents or guardians is required for minors under 14 years old. Data Controllers shall guarantee that they have confirmed, through effective means, the age of children and the authenticity of the consent provided, where applicable, by parents or guardians.
d. **Employee Consent**

Under the SDPA, consent must be: (i) freely given (which means that the Data Subject may not be compelled to provide his Personal Data, unless where expressly required by law); (ii) unequivocal (which means that no doubt exists as to the processing activities consented to by the Data Subject); (iii) specific (which means that the Data Subject must give his consent to each processing activity and for the purposes disclosed by the Data Controller); and (iv) informed (which means that the Data Controller has complied with its information requirements). In addition, according to general civil law principles, any consent provided by an individual by mistake, under intimidation, violence or willful misconduct will be void and null, particularly in employment relationships, where the employee is considered the weaker party. Labor courts have consistently indicated that consent provided under any of such circumstances will be void.

e. **Online/Electronic Consent**

Electronic consent is permissible and can be effective in Spain if properly structured and evidenced.

6. **Information/Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Subject; where the Personal Data is to be transferred; and how to access and/or correct the Data Subject’s Personal Data.

7. **Processing Rules**

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. **Rights of Individuals**

Data Subjects have the right to (i) request access to the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; (ii) request the correction of the Data Subject’s Personal Data; (iii) request the deletion and/or destruction of the Data Subject’s Personal Data; and (iv) object to further processing of the Personal Data.
9. Registration/Notification Requirements

Data Controllers are obliged to notify and register its Personal Data files before the Spanish DPA’s Registry. Registration must be performed prior to the use of any file or of any data processing operation. Any change of contents of the file or its use, including its cancellation, must also be notified. This obligation must be performed by means of the forms available at the Spanish DPA’s website and must be sent by the Data Controller in paper or electronically to the Spanish DPA.

10. Data Protection Officers (DPO)

There is no requirement for organizations to designate a data protection officer (DPO) or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

Transfers of Personal Data from Spain to countries offering an equivalent level of protection may take place freely. Said countries are EU and EEA Member States, Argentina, Israel, Andorra, Faroe Islands, Canada, Switzerland, Guernsey, the Isle of Man, Jersey, New Zealand, Uruguay and US recipients that have signed up to the Safe Harbor arrangement, and any other countries which are deemed to grant an equivalent level of protection under a decision of the European Commission. International transfers to third countries not granting an equivalent level of protection, such as the US (except as indicated above), may only take place under the SDPA where the prior authorization of the Spanish DPA has been obtained. Some exceptions to this requirement (i.e., where no authorization is required) are where:

- the Data Subject has given unequivocal consent to the transfer;
- the transfer is necessary for the performance of an agreement entered into between the Data Subject and the Data Controller or for taking pre-contractual measures at the Data Subject’s request;
- the transfer proves to be necessary for litigation purposes;
- the transfer is necessary for the conclusion or performance of a contract between the Data Controller and a third party to the benefit of the Data Subject;
- the transfer is in the public interest;
- the transfer is requested by tax and customs authorities; or
- the transfer is related to money transfers.

The transfer of Personal Data to a non-EEA country with inadequate protection levels is also permitted with the prior authorization of the Spanish DPA if a data transfer agreement is used and the agreement incorporates the
EU model contractual clauses for the transfer of Personal Data to third countries adopted by the European Commission on 15 June 2001 and 27 December 2004 (Data Controller to Data Controller) or on 5 February 2010 (Data Controller to Data Processor). The applicable EU model contractual clauses duly executed by the relevant parties (Data Exporter and Data Importer) are to be submitted, together with a transfer authorization request and additional documentation, to the Spanish DPA.

In addition, the prior authorization of the Spanish DPA may also be granted if the data transfer is based on Binding Corporate Rules (“BCRs”). In the process of authorizing the transfers based on BCRs, the Spanish DPA will review and comment on the BCRs.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

In accordance with the current law, a services contract (“Data Processing Agreement”) between a Data Controller and the service provider (“Data Processor”) to process Personal Data (e.g., payroll service) must include express restrictions that the Data Processor: (i) shall process the data only in accordance with the instructions of the Data Controller; (ii) shall not apply or use the Personal Data for any purpose other than that set out in the Data Processing Agreement; and (iii) shall not disclose the Personal Data to third parties. With respect to the third requirement, the DPAR now permits the Data Processor to subcontract data processing functions to a third party (“Subcontractor”), provided that the Data Processor obtains the Data Controller’s consent to engage the Subcontractor. Alternatively, the Data Processor may engage the Subcontractor if the Data Processing Agreement: (a) already specifies particular function(s) that may be subcontracted and names a pre-approved subcontractor; (b) requires that the Subcontractor process the Personal Data only in accordance with the Data Controller’s instructions; and (c) requires the subcontract to include terms providing for requirements (i) through (iii).

Where the Data Processor is located outside the EEA in a country not offering an equivalent level of protection, the Data Processing Agreement shall follow the model contractual clauses for the transfer of Personal Data to data processors located in third countries adopted by the European Commission.
14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, and/or private rights of action.

15. Data Security Breach

Presently, Data Controllers are not generally required either to notify the Spanish DPA or the Data Subjects upon the occurrence of a data security breach.

However, an amendment to the Spanish Telecommunications Act sets forth the obligation to notify the Spanish DPA and the Data Subjects, as applicable, of the occurrence of a data security breach where the Data Controller is an operator providing publicly available electronic communications services.

Notwithstanding any of the above, from an internal perspective, a data security breach or any anomaly which does or might affect data security (“Incident”) must be reported to the Data Security Officer or to the person appointed in the so-called security document drafted by the Data Controller or, where applicable, by the Data Processor. The Data Security Officer (or the appointed person) will then take the proper action to address the Incident and record the following details: (i) kind of Incident; (ii) the time at which it occurred; (iii) the person reporting it; (iv) to whom it was reported; and (v) the effects thereof.

An organization that is involved in a data breach situation may be subject to closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions, class actions, and/or a criminal prosecution.

16. Accountability

Organizations are required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline

Opinion 0128/2007 of the Spanish DPA (June 2007), entitled “Internal reporting schemes (whistle-blowing mechanisms)”, which is in line with Opinion 1/2006 of the Article 29 Working Party, generally foresees the establishment of whistle-blower hotlines dealing with accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. Although the implementation of whistle-blower hotlines exceeding the scope of Opinion 0128/2007 (e.g., sexual harassment, misconduct regarding the protection of the environment, inhumane working conditions, etc.) is not prohibited, it may be harder to implement the same as it
has to be accompanied with sufficient evidence to uphold the legitimacy and the need for the proposed processing.

Based on Opinion 0128/2007, it is advisable to submit specific filing requirements with the Spanish DPA as regards whistle-blower hotlines.

Data Controllers must inform employees about: the existence of the whistle-blower hotline and how it works.

Subject to certain exceptions, reported persons should be informed of the facts outlined by Opinion 1/2006 of the Article 29 Working Party, namely:

- entity responsible for the whistle-blower hotline;
- the facts surrounding the accusation;
- the departments or services which might receive the report within its own company or in other group companies; and
- how to exercise rights of access, rectification and cancellation.

Due to the novelty and complexity of a whistle-blower hotline and the sensitivity of the rights affected, there is no absolute guarantee from the Spanish DPA that even if the scheme is based on Opinion 0128/2007 of the Spanish DPA and Opinion 1/2006 of the Article 29 Working Party that it will be accepted without any further comments and/or amendments. In fact, the Spanish DPA requires the identification of the whistle-blower so anonymous reports are not accepted. This seems to be contradictory with Opinion 1/2006 of Art. 29 Working Party, which allows the filing of anonymous reports as an exception to the general rule, i.e. identified reports, in so far as anonymous reports are not expressly promoted. Based on several conversations with the Spanish DPA, the Spanish DPA’s position is that it will not accept the anonymous registration of any whistle-blower hotline in Spain.

18. E-Discovery

When implementing an e-discover system, an organization may be required to obtain the consent of employees if the collection of Personal Data is involved, and advise employees of the implementation of such system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace, and give employees the opportunity to review isolated emails designated as spam.
20. Cookies

On April 29, 2013, the Spanish DPA, together with industry representatives Adigital, Autocontrol, and IAB, published the Guide for the Use of Cookies in Spain (“Guide”). The document provides guidance for compliance with the general rule on installing and/or using cookies, which requires foremost informing and obtaining the consent of the user.

The Guide identifies cookies that are exempt from compliance with the general rule. These are cookies used (i) only to allow communication between the user and the network; or (ii) to provide strictly a service explicitly requested by the user, as well as “user-input” cookies, user authentication or identification cookies (for one session only) and security cookies, as well as other technical cookies used by plugins, provided that these are the sole purposes of the use of such cookies.

Thus, the installation and use of any other types of cookies remain subject to the general rule of informing and obtaining the user's consent. The Guide seeks to facilitate compliance with that rule by providing for the:

- **Duty to inform:** This entails providing clear and complete information regarding the use of cookies and their purposes/uses and how to revoke consent and remove cookies, making all these information available to users permanently, e.g. through a hyperlink to the Cookies Policy.

- **Duty to obtain consent:** This is the most controversial requirement since the legislation on cookies does not indicate whether the consent must be express or implied. The Guide states that it is always advisable to require users to mark a checkbox or click on an “I agree” button, since this can ensure that consent is properly obtained and will guarantee the provider’s ability to prove its compliance with the regulations on cookies. However, users will also be deemed to have provided their implicit consent if they should keep browsing the website, provided that:
  
i. users have performed a conscious and affirmative action;

  ii. users have been previously informed in an explicit, clear and unequivocal way as to the existence and purposes of the cookies used in the website; and

  iii. users are able to object to the use of cookies regardless of the potentially negative effects this may have on the browsing experience.

Therefore, owners of websites aimed at the Spanish market who have not already done so, should carry out a process of adopting these regulations by using this Guide as a reference. In this regard, we recommend from a practical point of view considering the implementation of the following measures:
• Reviewing and classifying the different cookies used by the organization under the new rules provided for in this Guide, and determining the information and consent requirements applicable to each type of cookie used;

• Modifying the information practices (entry page, banners, etc.) as well as the content of the information provided to the user (cookies notice, privacy policy, etc.); and

• Modifying, if necessary, methods and procedures for obtaining consent for the use of cookies.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.
Sweden

Sten Bauer
Stockholm
Tel: +46 8 566 177 16
sten.bauer@bakermckenzie.com

Johan Strand
Stockholm
Tel: +46 8 566 177 41
johan.strand@bakermckenzie.com
1. Recent Privacy Developments

**Camera Surveillance of Employees**

On 25 February 2015, the Swedish Data Inspection Board (the “Board”) announced that it will carry out a review of how retail businesses use camera surveillance to monitor employees. The Board states that there has been several reports in media regarding companies that use camera surveillance as a way to monitor employees and that the Board has also received indications that such camera surveillance is being carried out. Thus, the Board will carry out a wide review of how retail businesses are using camera surveillance in shop areas only accessible by employees.

In the first stage of the review the Board sent out surveys to a number of retail businesses containing questions regarding camera surveillance of employees. In the second stage, the Board selected a few retail business for a more detailed review. The review was completed by June 2015.

**Decision Regarding Use of Personal Data when Testing IT Systems**

On 15 September, 2014 the Board issued a decision against a train operator company that used personal data when testing a new IT system. In its decision the Board stated that the use of actual customer personal data in a testing environment can be in accordance with the Swedish Personal Data Act (1998:204) (“PDA”) if the customer can reasonably expect that such testing will be carried out. The Board further explained that it is more likely that customer personal data may be allowed to be used when testing the security of an existing system than in the development of a new system or new services in an existing system. However, the Board also stated that if fictitious or anonymized data can be used to carry out tests, such data shall be used instead.

In the case at hand, the Board found that the train operator had not used appropriate security measures in the testing environment to protect the personal data used in the tests. This had resulted in erroneous invoices and credit reports based on the personal data used in the testing environment. The Board was satisfied with the corrective measures taken by the train operator and therefore the Board did not take any further action.

**The Swedish Data Inspection Board Orders Municipality to Stop Using Cloud Services**

In 2011, the Board reviewed a Swedish municipality’s use of third party cloud services and found that it did not fulfill the requirements under the PDA. The Board criticized the data processor agreement for including provisions that allowed the cloud service provider to process the data for its own purposes and for not identifying the sub-contractors involved and what would happen to the data at the end of the agreement. The municipality was ordered to submit a new data processor agreement to the Board.
In June 2013, the Board reviewed the new data processor agreement submitted by the municipality. Once again the Board found that the agreement did not fulfill the requirements under the PDA. According to the agreement the cloud service provider would “process Customer Personal Data for the purposes of providing, maintaining and improving the services”. The Board found that this description of the purpose of the processing was too broad and did allow the cloud service provider to process data for its own purposes. Further, the agreement did not provide clear information on how long data was to be stored by the cloud service provider if the municipality ordered it to be deleted or after the end of the agreement. The Board also criticized the agreement for not providing the municipality with sufficient information regarding the identity and location of sub-contractors who could come to process data under the agreement. The decision was appealed to the Administrative Court by the municipality and the cloud service provider. On 1 July 2014, the Administrative Court denied the appeal.

The Board is currently reviewing another municipality’s data processor agreement with the same third party cloud services provider. The Board is expected to issue its decision during the second quarter of 2015.

**Checklist for Data Processing Using Mobile Devices**

The Board has released a checklist on how to comply with the PDA when processing personal data using mobile devices such as tablets and smartphones. The checklist is only provided as non-binding guidance. The list includes the following:

- conduct a risk analysis to identify the specific risks involved when using mobile devices;
- train and inform the users of the mobile devices so that they know how personal data may be handled, what security settings to use, limitations on private use, what apps they are allowed to download, and the consequences of prohibited use;
- implement an authorization system which only allows the users in need of specific information access to that information;
- use authentication and encryption to protect data transferred over the Internet;
- data stored on mobile devices should be encrypted and not unintentionally stored by cloud services;
- use security measures such as password screen locks, remote locking, and control in case of theft and automatic locking after a certain period of inactivity;
- log usage and follow up on who has accessed the device;
limit access to personal data on mobile devices;

- enter into a data processor agreement when using third parties to process data; and

- stay up to date with the latest technology in order to understand the security measures needed for new applications and services.

2. Emerging Privacy Issues and Trends

- **Cloud Computing** - Although the use of cloud services is not a new phenomenon in Sweden, the decisions by the Board regarding municipalities’ use of cloud services raises questions among municipalities who want to use cloud services. The Board is continuing to review cloud service agreements that municipalities have entered into. The Board’s latest review of a cloud service agreement entered into by a municipality is planned to be completed during the second quarter of 2015. Critics have expressed concern that the Board’s interpretation of the PDA is in conflict with the realities related to the provision of cloud services.

- **Camera Surveillance** - The Board will focus on retail businesses’ camera surveillance of employees during the first half of 2015. The result of the review will likely provide guidance for companies in other sectors regarding the use of camera surveillance of employees.

3. Scope of the Law


Camera Monitoring Act (2013:460) (“CMA”), governing privacy and use of camera monitoring.


Credit Information Act (1973:1173), which contains privacy regulations in relation to credit information.


Patients’ Personal Data Act (2008:355), which governs the processing of personal data in the healthcare sector.
4. Key Privacy Concepts

a. Personal Data
The PDA applies to the processing of any information (“Personal Data”) relating to an identified or identifiable living individual (“Data Subject”).

b. Data Processing
“Processing” is widely defined and covers any operation or set of operations performed on Personal Data, including, inter alia, collection, recording, organization, storage, transfer and deletion. The PDA applies to both manual and automated data processing. However, the processing of Personal Data in non-structured formats (e.g., in running text or the use of ordinary e-mail programs), is subject to exemptions from many of the rules under the PDA, including the requirements set out with respect to the processing of sensitive Personal Data and transfer of Personal Data to a country located outside of the EEA. Notwithstanding, the exceptions only apply if the processing does not give rise to any violation of the Data Subject’s personal integrity.

c. Processing by Data Controllers
The PDA applies to those persons who, alone or together with others, determine the purposes for which and the manner in which any Personal Data is processed (“Data Controller”).

d. Jurisdiction/Territoriality
The PDA applies to data processing activities carried out by Data Controllers established in Sweden; and Data Controllers that are not established in the EEA but use equipment based in Sweden to carry out data processing activities (other than merely for the purpose of transit).

e. Sensitive Personal Data
The PDA imposes additional requirements on the processing of sensitive Personal Data – that is, Personal Data relating to race or ethnic origin, political opinions, health or sex life, religious or philosophical beliefs and membership of a trade union. Specifically, the processing of sensitive Personal Data is prohibited, unless certain conditions are met, including:

- the Personal Data has been made public by the Data Subject or the Data Controller obtains the explicit consent of the Data Subject (see Section 5(b));
- the processing is necessary to carry out the obligations and rights of the Data Controller in the field of employment law;
- the processing is necessary to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent;
• the processing is carried out in the course of legitimate activities with appropriate guarantees by a foundation, association or any other non-profit seeking body with a political, philosophical, religious or trade union aim and provided certain conditions are met;

• the processing is necessary for the establishment, exercise or defense of legal claims;

• the processing is performed by a health care professional for certain purposes or under an obligation of secrecy within the medical advice or treatment area; or

• the processing is performed for research and statistical purposes, provided the public interest in the research or statistical project clearly outweighs the risk of undue violation of the Data Subjects’ integrity.

The PDA imposes additional requirements on the processing of personal identification numbers as well as Personal Data concerning violations of the law. In principle, it is, with a few exemptions, prohibited for any entity other than government authorities to process Personal Data relating to crime, suspicion of crime and criminal judgments. Personal identification numbers may be processed only when it is clearly necessary having regard to the purpose of the processing; the importance of a certain identification; or any other considerable reason.

f. Employee Personal Data

Employee Personal Data is likely to include both non-sensitive Personal Data and sensitive Personal Data (e.g., health-related information). Sensitive employee Personal Data may be processed under the circumstances mentioned in Section 4(e) above, commonly for the purpose of carrying out the Data Controller’s obligations in the field of employment law. Non-sensitive employee Personal Data may be processed by a Data Controller for purposes that are necessary in order to maintain and administer the employment relationship (e.g., performing a contract to which the Data Subject is a party, or carrying out the Data Controller’s legal obligations). Other justifications for processing non-sensitive employee Personal Data may include purposes which are of legitimate interest of the Data Controller and which are considered to be of greater weight than the Data Subject’s interest in his or her protection of the personal integrity. A fallback justification for processing both sensitive and non-sensitive Personal Data in the employment context may be if consent is provided by the Data Subject. However, there are limitations on what is considered to constitute valid consent in the employment context (see Section 5(d) below).
5. Consent

a. General

As a general rule, personal data may be processed only if the Data Subject gives consent. There are a number of exceptions to this requirement, which legitimize processing without the consent of the Data Subject. Nevertheless, consent is, in practice, often one of the more straightforward ways of justifying processing. Written consent is not required. However, it is worth noting that, when in dispute, it is the Data Controller that is required to demonstrate that consent has been obtained. There is no language requirement set out in the PDA. However, the Board requires that all information provided to Data Subjects regarding consent of processing Personal Data shall be translated into Swedish. If the Data Subject is proficient in the alternative language, it could nevertheless be argued that a translation is unnecessary.

b. Sensitive Data

Where consent is relied upon to justify the processing of sensitive Personal Data, it must be explicit. Written consent is not expressly required but may be preferable in order to prove that consent has in fact been obtained.

c. Minors

Although the PDA does not expressly regulate the Data Subject’s right to consent to the processing of his or her Personal Data, it is generally accepted that persons having reached the age of 15 years normally can provide valid consent. However, the situation must be assessed on a case-by-case basis. Valid consent is usually determined based on whether or not the Data Subject is capable of understanding the implications and effects of the consent, depending on, inter alia, the Data Subject’s age, the purpose of the processing and the Personal Data to be processed. If a Data Subject who is a minor is not considered to be able to give valid consent, a parent or legal guardian must provide consent on the Data Subject’s behalf.

d. Employee Consent

The Board has produced an opinion on the processing of Personal Data in the employment context. The Board’s view is that consent is not freely given where there is a real or a potential prejudice arising from not consenting or where there is no real possibility for the employee to refuse to give his or her consent. The Board goes on to state that if an employee is genuinely able to withdraw his or her consent at any time without suffering any detriment, this is an indication that the consent is freely given.

e. Online/Electronic Consent

Consent may be given electronically and will be considered to have been sufficiently demonstrated where it can be shown that the Data Subject had sufficient notice of the requisite information forming the basis of consent (e.g., inclusion of a hyperlink to a notice or policy directly above a consent
button) and steps have been taken to prevent consent from being mistakenly given (e.g., a double click acceptance process). Note that guidance has not been issued on the interrelated issue of how to verify that it is the correct Data Subject who consents to the processing.

6. Notice Requirements

An organization that collects personal data must provide data subjects with information about: the organization’s identity, the purposes for collecting personal data, its privacy practices (which must be given in a clear and transparent way), third parties to which the organization will disclose the personal data, the consequences of not providing consent, the rights of the data subject, where the personal data is to be transferred and stored, how to contact the privacy officer or other individual who is accountable for the organization’s policies and practices, how to make an inquiry or file a complaint, and how to access/and or correct the data subject’s personal data.

7. Processing Rules

An organization that processes personal data must limit the use of the personal data to only those activities which are necessary to fulfill the identified purpose(s) for which the personal data was collected, and delete/anonymize personal information once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data subjects have the general right to: be informed by an organization of the personal data the organization holds about the data subject, be informed by an organization of how the data subject’s personal data is being processed, request the correction of the data subject’s personal data, and request the deletion and/or destruction of the data subject’s personal data.

9. Registration/Notification Requirements

The Controller is subject to a general notification duty to the Board regarding the Personal Data processing activities performed by the Controller. The notification shall be made on a special form in Swedish, but the information to be provided is not very detailed. There are certain exemptions from the notification duty, i.e., (i) valid consent to the processing is obtained; (ii) a Data Protection Officer has been duly appointed (see Section 10); or a certain record on the Personal Data processing activities is held by the Controller (not applicable to sensitive Personal Data).

10. Data Protection Officers

It is not mandatory to appoint a Data Protection Officer (“DPO”) but some Controllers do so in lieu of notifying the Board (see Section 9) and/or to get some support and point of contact with respect to the Personal Data activities. The DPO shall be (i) sufficiently familiar with Swedish data privacy laws; and
(ii) independent of management. It is recommended by the Board (but not legally) required that the DPO speaks Swedish and lives in Sweden. The DPO does not need to be employed by the Controller. The Controller shall notify the Board of the DPO appointment on a specific form in Swedish.

11. International Data Transfers

Subject to the specific exceptional authorizations below, Personal Data may not be transferred to third countries (i.e., countries outside the EEA) unless the destination country provides for “adequate protection” of the Personal Data or pursuant to one of the following exceptions:

- the Data Subject has given his or her express consent to the transfer;
- the transfer is for the performance of a contract between the Data Subject and the Data Controller of Personal Data or the implementation of pre-contractual measures taken due to a request of the Data Subject;
- the transfer is for the conclusion or performance of a contract between the Data Controller and a third party which is in the interest of the Data Subject;
- the transfer is for the establishment, exercise or defense of legal claims; or
- the transfer is for the protection of vital interests of the Data Subject.

Transfers of Personal Data from Sweden to certain third countries that have self-certified with the Safe Harbor Privacy Principles arrangement are generally permitted, since these countries and arrangements are considered as providing adequate protection. Moreover, the use of a data transfer agreement incorporating the model clauses adopted by the European Commission will legitimize a transfer of Personal Data to non-EEA countries without adequate protection. Prior notification of the agreement to the Board is not required. Another alternative which will legitimize a transfer of Personal Data is if binding corporate rules are implemented. However, this alternative is normally fairly time consuming.

12. Security Requirements

Organizations are required to: take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.
13. Special Rules for Outsourcing of Data Processing to Third Parties

A transfer of Personal Data must as a general rule be necessary for the purpose of the processing. Organizational, cost efficiency, and security reasons are normally viewed as acceptable reasons for a transfer of Personal Data due to outsourcing. Although the Personal Data processing is outsourced, the Controller remains responsible for the processing activities. Consequently, the Controller must make sure that the provisions under the DPA and other related regulations are complied with, both by the Controller but also by the third party service provider. The third party service provider and its sub processors (if any) are viewed as Processors, implying that the written processor agreement obligation would be triggered (see Section 7). Moreover, should Personal Data be transferred to a country located outside of the EEA, the Controller must make sure that any of the exceptions to the general prohibition on transferring Personal Data to a third country applies or that another acceptable measure for the transfer has been taken (see Section 11). The Controller may be obliged to provide the Data Subjects with information about the transfer of their Personal Data.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

The law is somewhat unclear in this respect and there are no specific statutory provisions regulating the subject matter, but according to the Board, the Controller shall normally inform Data Subjects of the breach. The information shall, inter alia, include details about the anticipated effects of the breach. Moreover, the Controller shall inform other institutions that might be affected, (e.g., banks). There is no obligation to notify the Board. However, if large numbers of people are affected, it might be advisable to contact the authority.

An organization that is involved in a data breach situation may be subject to closure or cancellation of the file, register or database; an administrative fine, penalty or sanction; civil actions and/or class actions; and/or criminal prosecution.

16. Accountability

Organizations are required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data, and, upon request, furnish the results of the
privacy impact assessments and/or evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

17. Whistle-blower hotline
There is no filing requirement for the introduction of a whistle-blower hotline, but certain limitations with respect to the use of the whistleblower hotline apply. Moreover, the ordinary notification duty applicable with respect to the normal course of processing of Personal Data will still apply (see Section 9).

18. E-discovery
It is generally permissible to process Personal Data for the individual control of employees’ use of e-mail and Internet for the purposes of litigation or regulatory requests, provided that the Controller complies with the rules of the PDA. Further, employers must provide employees with detailed information about: the implementation of the e-discovery system, the purpose of the processing, the monitoring of work tools (e.g., e-mail, Internet), and the storage of inter alia e-mails. In general, employers are not entitled to review and process any of the employees’ private information. According to the Board, it is advisable to implement an Internet-policy that contains guidelines for the employee use of Internet and e-mail.

19. Anti-Spam Filtering
Generally, the introduction of a spam filtering solution in an organization does not raise privacy issues provided the employees have agreed to the spam filtering solution or have the possibility to access the e-mails that have been filtered. However, the individual control of such a spam filtering system will raise privacy issues (see Section 17).

20. Cookies
There are specific laws/rules that regulate the deployment of cookies, and hence, the use of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.
Switzerland

Nicolas Passadelis
Zurich
Tel: +41 44 384 1209
nicolas.passadelis@bakermckenzie.com
1. Recent Privacy Developments

On 14 January 2015, the Federal Supreme Court ruled that Article 32 of the Convention on Cybercrime ("CCC") does not permit Swiss public prosecution authorities to access or receive computer data stored in another country without first obtaining lawful and voluntary consent of the person who has the lawful authority to disclose the relevant computer data. A Swiss public prosecution authority investigating an alleged violation of applicable anti-racism legislation by way of a social media post had ordered an US-based social media provider to disclose the social media account details and traffic data relating to the relevant post. In addition, it requested that the competent Compulsory Measures Court permit the implementation of surveillance measures relating to the social media account from which the relevant posted originated. Compulsory Measures Court, however, rejected the request by its decision dated 27 August 2014. The public prosecution authority unsuccessfully appealed against this decision before the Federal Supreme Court.

The Federal Supreme Court acknowledged that the purpose of Article 32 CCC was to grant under certain circumstances a member state the right to access or receive data located in another member state without having to resort to (usually lengthy) mutual legal assistance proceedings. In the case at hand, however, the Federal Supreme Court that neither of the access rights provided for in Article 32 CCC applied in the case at hand. More specifically, it ruled out Article 32 let. a CCC because the data requested by the Swiss public prosecution authority was not public. The Federal Supreme Court also denied the application of Article 32 let. b CCC because the social media provider had not agreed to provide the requested information to the Swiss public prosecution authority despite the fact that the social media provider would have had the right to do so based on its general terms and conditions. In fact, the social media provider had declared that they would only provide the data if they were legally compelled to do so. The Federal Supreme Court found that the position expressed by the social media provider could not be interpreted as consent as contemplated under Article 32 let. b CCC. It, therefore, rejected the appeal.

This ruling is important because it strengthens the principle of territoriality in connection with information access requests. According to this principle, public prosecutors can only enforce their local laws against service providers domiciled in the same jurisdiction. If the relevant authority wants to gain access to information hosted by service providers domiciled abroad, it must resort to mutual legal assistance proceedings unless the relevant information is public or the service provider is legally entitled and agrees to provide such information.
2. Emerging Privacy Issues and Trends

In April 2015, the Federal Council decided to amend the Federal Data Protection Act. To that end, it instructed the Federal Department of Justice and Police to submit a draft amendment by end of August 2016 with the intention to strengthen the protection of personal data in Switzerland. Since 2010, data protection law in Switzerland was under scrutiny. A report released in late 2011 concluded that data protection must be strengthened to meet the increasing challenges triggered by technological and social developments. In the wake of this report, the Federal Council asked the Department of Justice and Police to evaluate which legislative measures should be taken to increase the effectiveness of the Federal Data Protection Act. The Department of Justice and Police submitted its evaluation report on 29 October 2014 which will serve as a basis for drafting the proposed amendments. These amendments will take into account legislative data protection initiatives in the European Union as well as the Council of Europe.

3. Law Applicable

The FLDP as implemented by the Federal Ordinance on the Federal Law on Data Protection of June 14, 1993 (“Ordinance”).

The FLDP and the implementing Ordinance were substantially revised in 2007. The revised provisions entered into force on January 1, 2008. Besides delivering greater transparency through stricter information obligations regarding Sensitive Personal Data and Personality Profiles, the revision resolves some existing contradictions in the language and also introduces some incentive for self-regulation. Switzerland is not subject to the European Union’s Data Protection Directive (95/46/EC).

4. Key Privacy Concepts

a. Personal Data

The FLDP applies to the processing of any information (“Personal Data”) relating to an identified or identifiable legal person or natural person (“Data Subject”).

b. Data Processing

“Processing” is broadly defined in the FLDP and includes all acts relating to Personal Data, regardless of the equipment and procedures used, in particular the collection, storage, use, modification, disclosure, archiving or destruction of Personal Data. The FLDP applies to both automated and manual data processing.
c. Processing by Data Controllers
The FLDP applies to those persons who determine the purposes for which and the manner in which any Personal Data is, or is to be, processed (“Data Controller”).

d. Jurisdiction/Territoriality
The FLDP applies to Data Controllers domiciled in Switzerland, and the processing of Personal Data pertaining to Data Subjects domiciled in Switzerland.

e. Sensitive Personal Data
The FLDP imposes additional requirements for the processing of Sensitive Personal Data – that is, Personal Data concerning religious, philosophical, political or union opinions or activities; health, sexuality or racial origin; social security files; and criminal or administrative proceedings and sanctions. In addition, special rules apply to “personality profiles.” A personality profile is a collection of Personal Data that allows for the appraisal of the essential characteristics of an individual’s personality (“Personality Profile”).

The amended FLDP provides for an obligation to register data collections with the Data Protection Commissioner if (i) the Data Controller regularly processes Sensitive Personal Data or Personality Profiles, or (ii) it regularly discloses Personal Data to third parties (including other group companies). By way of exception, the Data Controller will not have to register if (among other things) it has appointed an internal data protection commissioner who independently supervises the compliance with the data protection legislation and who keeps a register for all the data collections. Therefore, by appointing an internal data protection commissioner, the Data Controller can avoid having to register under the amended laws.

The processing of Sensitive Personal Data is prohibited unless justified by the consent of the Data Subject, an overriding public or private interest, or the law (see Section 7 below). These criteria will be applied in a stricter manner if there are Sensitive Personal Data or Personality Profiles involved. The revised law introduces the obligation of the Data Controller to actively inform the Data Subjects about the collection of Sensitive Personal Data or Personality Profiles. This information must at least cover the identity of the Data Controller, the purpose of the processing, and the categories of recipients of the Personal Data (if it is intended to disclose the Personal Data to third parties).

f. Employee Personal Data
Employee Personal Data is likely to include Sensitive Personal Data (e.g., health-related information) and non-sensitive Personal Data. The processing of the employees’ Personal Data, whether sensitive or non-sensitive will be justified if required to implement an employment agreement. Other justifications may be invoked under certain circumstances.
5. Consent Requirements

a. General
The consent of the Data Subject is not mandatory, although it is contemplated as a justification for the processing (see Section 7 below) as well as cross-border transfers (see Section 11 below) of Personal Data. In practice, it is often one of the more reliable ways to justify any data processing. Written consent is not required but is recommended for evidential purposes.

b. Sensitive Data
The FLDP does not distinguish between Sensitive and non-sensitive Personal Data as regards consent requirements. However, a court may in practice apply stricter criteria to the consent language in connection with the processing of sensitive Personal Data than with the processing of non-sensitive Personal Data. The revised law requires the explicit consent of the Data Subject if the processing involves sensitive Personal Data or Personality Profiles.

c. Minors
Persons under the age of 18 cannot give valid consent. A parent or legal guardian must give consent on their behalf.

d. Employee Consent
An employee’s consent will be valid only if it is freely given prior to the processing of the Personal Data. This requirement will not be fulfilled if consent is given by the employee to avoid a real or potential prejudice which could arise from not consenting, where there is no real possibility of the employee refusing to consent, or where the consequence of refusal is that a candidate will not be offered employment. Where the employee or the candidate is entitled to withdraw its consent at any time without suffering any detriment, this is an indication that consent is freely given. An employee’s consent can be given explicitly or tacitly. A tacit consent will not suffice if the processing involves sensitive Personal Data or Personality Profiles.

e. Online/Electronic Consent
Consent may be given electronically, and will be considered to have been sufficiently demonstrated where it can be shown that the Data Subject had sufficient notice of the requisite information forming the basis of consent (e.g., inclusion of a hyperlink to a notice or policy directly above a consent button) and steps have been taken to prevent consent from being given mistakenly (e.g., a double click acceptance process).

6. Information/Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity, the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy policies (which
must be given in a clear and transparent way); third parties to which the
organization will disclose Personal Data; where the Personal Data is to be
transferred; how to contact the privacy officer or other person who is
accountable for the organization’s policies and practices; how to make an
inquiry or file a complaint; and how to access and/or correct the data subject’s
Personal Data.

7. Processing Rules
An organization that processes Personal Data must limit the use of Personal
Data to only those activities which are necessary to fulfill the identified
purpose(s) for which the Personal Data was collected; and delete/anonymize
Personal Data once the stated purposes have been fulfilled and legal
obligations met.

8. Rights of Individuals
Data Subjects have the general right to: access the Data Subject’s Personal
Data subject to some restrictions and/or qualifications; request the correction
of the Data Subject’s Personal Data; and request the deletion and/or
destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements
An organization that collects and processes Personal Data may be required to
register, and notify the appropriate data authority. See Section 4(e) for the
obligation to register data collections with the Data Protection Commissioner
under certain circumstances.

10. Data Protection Officers
In Switzerland, there is no requirement to appoint or designate a data privacy
officer or other individual who will be accountable for the privacy practices of
the organization.

11. International Data Transfers
Personal Data may not be transferred abroad if such transfer could put the
Data Subjects at risk. The personality of the persons affected will be
particularly put at risk if the data is transferred to countries that fail to provide
a level of protection equivalent to the level provided under Swiss law. The
Swiss Federal Data Protection and Information Commissioner keeps a list of
countries deemed to provide an equivalent level of protection. The EU
member states are included in this list. The revised law introduces a catalogue
of reasons which justify the transfer of Personal Data to countries that lack an
adequate level of data protection. This catalogue is exhaustive, i.e., the
transfer of Personal Data to such countries is only lawful if one of these
reasons for justification is fulfilled. In order to prevent putting the persons
concerned at risk, the Data Controller can, for instance, require the data
recipient to sign a data transfer agreement or obtain the Data Subject’s consent to the transfer.

An organization may transfer Personal Data outside of the jurisdiction provided that: appropriate data transfer agreements (i.e., Model Contractual Clauses) or other prescribed measures are put in place; binding corporate rules (“BCRs”) are implemented to secure international data transfers; or recipients in the US are registered under the Safe Harbor agreement.

12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for the Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties may potentially be required to use contractual or other means to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors. In case of an occurrence of data breach, the outsourcing organization will be held liable together with the third party provider.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
There is no explicit provision in the FLDP that would require the Data Controller to notify the Data Subjects or the Data Protection Commissioner in the event of a data security breach. However, one of the aims pursued by the revisions to the FLDP was to enhance the transparency in the processing of Personal Data. One of the provisions introduced as part of the new law requires that the data collection and the purpose thereof be noticeable by the Data Subject. Taking into consideration that the Data Subject must know about any collection of its data, one could certainly argue that this requirement also applies to security breaches because a security breach logically leads to the data being collected by a third party. Notification may also be contractually required if there is an agreement between the Data Controller and the Data Subject explicitly or implicitly imposing a notification obligation on the relevant organization.
Organizations that have suffered a data security breach must determine on their own whether and what kind of action to take in response to the breach. The organization must, therefore, decide on a case-by-case basis whether to notify in the event of a data security breach. To that end, the organization may seek guidance from the competent authorities on an informal basis. There is no formal procedure for informal consultations with the authorities.

This decision on whether or not to notify may depend on the nature of the data concerned. While Swiss laws do not formally distinguish between sensitive and non-sensitive information in connection with data security breaches, it is important to highlight that the statutory requirements will be applied more strictly if sensitive data are involved. A notification is more likely to be required if sensitive data are affected by the data security breach.

The impact of a data security breach that becomes public on organizations can be manifold. The security breach can trigger an investigation by the Federal Data Protection and Information Commissioner. Violating data protection obligations may also result in civil liability. The Data Subject may sue the organization for correction, cease and desist, deletion, and damages covering financial losses or lost profits incurred by the Data Subject. The damages depend on the actual losses and lost profits proved by the Data Subject. In very exceptional cases, the Data Controller may have the obligation to pay a satisfaction amount to the Data Subject to compensate immaterial damages. Finally, data security breaches and investigations may entail publicity and, therefore, cause reputational harm.

16. Accountability

There is no existing law in Switzerland that requires organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. It is also not a requirement to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

17. Whistle-blower Hotline

No filing requirement is required other than the regular data protection filings, provided that the criteria for such filing are met.

18. E-discovery system

There are no requirements that apply other than the general legal requirements under the Swiss data protection law and, potentially, labor law.

19. Anti-spam filter

There are no requirements that apply other than the general legal requirements under the Swiss data protection law and, potentially, labor law.
20. Cookies
The use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. The organization may be required to obtain consent for a specific activity as bundled consent may not be considered valid consent.
Taiwan

H. Henry Chang
Taipei
Tel: +886 2 2715 7259
henry.chang@bakermckenzie.com

Chris Tsai
Taipei
Tel: +886 2 2715 7310
chris.tsai@bakermckenzie.com
1. Recent Privacy Developments

The Personal Data Protection Act (“PDPA”) of 2010, which replaced the previous Computer-Processed Personal Data Protection Law (“CPPDPL”) of 1995, came into effect on October 1, 2012, save for two particularly controversial articles (Articles 6 and 54- Please see Section 3.). The PDPA is the only existing law that expressly regulates automated Personal Data collection and transmission. It applies to both public and nonpublic institutions. The previous provisions relating to the requirement of government approval/license under the CPPDPL have been revoked. One of the main requirements for regulated non-public institutions is that they must obtain the Data Subject’s prior written consent in order to process Personal Data, and they must have a predefined purpose for collecting such data.

2. Emerging Privacy Issues and Trends

Overhaul of Taiwan’s Data Protection Law

By comparison to its predecessor, the PDPA has significantly tightened the Personal Data protection laws in Taiwan and has already changed the ways in which Personal Data can be collected, processed, stored, used and transmitted.

Under the PDPA, Data Collectors are required to give affirmative notice to the Data Subjects whose Personal Data they collect and must advise them of the purposes for which their Personal Data is being collected or used, as well as the sources from which the data is derived.

The PDPA also provides for stiffer civil and criminal penalties if individuals or enterprises profit from the collection, processing or use of Personal Data.

Personal Information File Security Maintenance Plan for Non-government Agencies

Article 27 of the PDPA requires non-government agencies to adopt proper security measures in retaining Personal Data. Since the implementation of the PDPA in October 2012, various industries have implemented their respective rules for Personal Information file security maintenance plan, such as the multi-level marketing industry, human resources recruitment industry, real estate agents, water corporations, non-government agencies designated by the Financial Supervisory Commission (“FSC”) (including financial holding companies, banking industry, securities industry, futures industry, insurance industry, institutions that engage in electronic stored value cards, foundations that are under the FSC regulations), and tourist hotel enterprises. Each enterprise covered under its respective industry shall adopt the proper security measures in retaining the collected Personal Data and report to the competent authorities for record. Thus, it is foreseeable that it will become a common practice for companies to implement much more organized and established Personal Information Files Maintenance Plan.
Data Protection Enforcement

Since the implementation of the PDPA on October 1, 2012, there have only been a few cases where competent authorities have imposed penalties, whether civil, criminal or administrative, on public and nonpublic institutions pursuant to the PDPA articles. There are various financial institutions, including banks and insurance companies, that have been fined by the FSC (the competent authority of financial institutions) for violating the data protection requirements based on their respective regulations, such as the Banking Act and the Insurance Act. The financial industry is a highly regulated industry and the penalties set forth in those applicable regulations are much higher than those in the PDPA. Also, when it comes to data protection, financial-related statutes and regulations are special laws compared to the PDPA and thus trump the application of the PDPA.

Anti-Spam Legislation

In February 2009, the government introduced an anti-spam bill called the Commercial Electronic Mail Management Act (“Bill”). The Bill, which is still in the legislative process, defines unsolicited email or spam as email intended to market commercial products or services which are not based on an existing relationship between the sender and the recipient. The Bill seeks to reduce the burden of commercial emails by introducing (i) consumer consent and other requirements with which commercial email senders must comply with, and (ii) by giving spam recipients the right to recover damages.

Under this Bill, spam will be considered legitimate only if the recipient consents to receiving it. The law will authorize a sender (a legal entity, group or individual who initiates commercial email) to send an initial unsolicited commercial email, provided the email is clearly marked as a commercial advertisement, contains the sender’s name and business address and gives the recipient an opt-in option to receive subsequent messages from the sender. The recipient’s failure to respond to the sender’s initial email constitutes that recipient’s refusal to receive the sender’s subsequent messages. The Bill will also prohibit most forms of randomly generated spam, including those that harvest email addresses derived from alpha-numeric searches.

If passed and promulgated as expected, the Bill will give spam recipients a right to recover NT$500 to NT$2,000 (approximately US$17 to US$69) from the sender for each unauthorized commercial email. It will also authorize class action lawsuits by authorized organizations on behalf of at least 20 persons.

An early version of Taiwan’s proposed anti-spam legislation was criticized because it imposed heavy obligations on internet service providers by requiring them to implement specific measures to prevent commercial email abuses.
As of August 2015, this Bill is still under review by the commission of the Legislative Yuan.

There is no new development on the Bill or its proposed amendments.

3. Law Applicable

Specific data protection rules can be found in: (i) the PDPA, which regulates all individuals and legal entities that collect, use or process Personal Data and (ii) the constitutional right to privacy recognized by the Council of Grand Justices, which protects an individual’s ability to control his or her own Personal Data, including control over whether to disclose Personal Data, the time, manner and scope of disclosure and the right to correct such information when it is wrongly stated.

This right to privacy is present in various laws and regulations of Taiwan:

- the Civil Code of Taiwan provides a private right of action for the tortuous infringement of privacy;
- the Freedom of Government Information Law prohibits the release of government information that will result in an invasion of personal privacy;
- the Criminal Code penalizes certain types of privacy infringements, including eavesdropping, illegally opening sealed envelopes, and unauthorized release of privileged medical, financial or legal information; and
- the Guidelines for Consumer Protection in E-Commerce apply to business operators in electronic commerce. While the Guidelines are not formal law, they may be legally enforced under the provisions of Taiwan’s Consumer Protection Law. They include Guidelines for collecting, using and protecting consumers’ Personal Data.

**PDPA articles that are still pending**

Article 6 of the PDPA specifically regulates the collection, processing and use of Sensitive Personal Data, which include information on medical treatment, genetics, sexual life, health examination and criminal record. Such Sensitive Data cannot be collected, processed, or used unless under limited exceptions. The exceptions do not include the individual’s consent.

This Article has been widely criticized as it is generally considered to be overly-rigid and unreasonable.

Article 54 requires that, if an agency holds Personal Data collected prior to October 1, 2012 that was not provided directly from the individual concerned (but from a third person or source), the agency is required to procure and obtain the consent of the individual concerned within one year from October 1,
2012. The requirement of Article 54 is expected to impose major compliance difficulties, which would result in heightened compliance costs.

As of August 2015, these two articles are still pending and are not yet effective. Some amendments to other articles of the PDPA were proposed and sent to the Legislative Yuan for further discussion; however, no new developments are underway.

4. Key Privacy Concepts

a. Personal Data
Under the PDPA, “Personal Data” means a natural person’s name, date of birth, national identification number, passport number, special features, fingerprints, marriage, family, education, occupation, medical records, medical history, genetic information, sex life, health examinations, criminal records, contact information, financial status, social activities, and other data sufficient to directly or indirectly identify the said person.

b. Data Processing
The PDPA defines data processing as recording, inputting, storing, editing, amending, correcting, copying, retrieving, deleting, outputting, or transmitting Personal Data collected in order to create or use the personal profile of a Data Subject.

c. Processing by Data Controllers
The applies to public institutions, all individuals, legal entities and enterprises that collect, use or process Personal Data.

d. Jurisdiction/Territoriality
The PDPA extends to:

- the collection, use or processing of Personal Data in Taiwan by all individuals, legal entities and enterprises (including Taiwan and foreign individuals, legal entities and enterprises);
- the collection, use or processing of Personal Data of Taiwan citizens by all individuals, legal entities and enterprises outside of Taiwan; and
- the international transmission of Personal Data by all individuals, legal entities and enterprises.

e. Sensitive Personal Data
The PDPA will impose stricter requirements for Sensitive Personal Data including medical information, genetic information, sex life, health examinations and criminal records so that they are subject to a higher level of protection. These kinds of Personal Data are banned from being collected, processed or used, except under limited circumstances. However, this provision is not effective yet (see 5(b) below).
f. Employee Personal Data

The PDPA treats employee Personal Data the same way as other Personal Data. Labor laws do not address employee Personal Data.

5. Consent

a. General

Under the PDPA, public institutions may, but are not required to, obtain the Data Subject’s consent when they act within the scope of their official responsibility or when there is no likelihood of injury to the Data Subject’s rights and interests.

Under the PDPA, in principle and subject to certain exceptions, non-public institutions must (i) have a predefined purpose, and (ii) meet certain requirements prescribed by the law in order to process Personal Data.

With respect to the Guidelines for Consumer Protection in E-Commerce, business operators engaged in electronic commerce should obtain the consumers’ consent before collecting or processing their Personal Data. Note that businesses should obtain parental consent before collecting, using or revealing to a third party any information respecting the Personal Data of children under 12 or their family members.

b. Sensitive Data

The PDPA will impose stricter requirements for sensitive personal data including medical information, genetic information, sex life, health examinations and criminal records so that they are subject to a higher level of protection. These items of Personal data are banned from being collected, processed or used except under limited circumstances. However, this provision is not yet effective.

c. Minors

Minors under the age of 20 cannot give valid consent, except with respect to matters within the normal everyday life of a minor. The parent or legal guardian of a minor may consent on behalf of the minor. A parent or legal guardian may validate a contract made by a minor who has reached the age of 7 but is under the age of 20.

d. Employee Consent

No special rules apply for employee consent, though it is understood that employee consent is not required to carry out an employment contract or administer an employment relationship.

e. Online/Electronic Consent

Consent may be given electronically via a qualified electronic signature pursuant to the Electronic Signature Act.
6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity, the purposes for collecting Personal Data, third parties to which the organization will disclose the Personal Data, the consequences of not providing consent, the rights of the Data Subject, how to make an inquiry or file a complaint, how to access/and or correct the Data Subject’s Personal Data, and the duration of the proposed processing.

7. Processing Rules
An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/ anonymize personal information once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications, request the correction of the Data Subject’s Personal Data, and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements
There is no registration requirement under the PDPA. When the Personal Data is stolen, disclosed, altered or infringed caused by the violation of the PDPA, the collector should notify the Data Subject.

10. Data Protection Officers
Under the new PDPA, public institutions must designate personnel who are exclusively responsible for data protection. Non-public institutions must take appropriate measures to prevent Personal Data from being stolen, amended, destroyed or disclosed.

11. International Data Transfers
Under the PDPA, the central competent authority may restrict international transmission of Personal Data by non-public institutions in any of the following circumstances:

- such transmission involves major national interest;
- such transmission is subject to special provisions of an international treaty or agreement;
the receiving country lacks proper laws and regulations that adequately protect Personal Data, and the rights and interests of a Data Subject are likely to be injured/damaged; or

• Personal Data is indirectly transmitted to a third country (area) to evade the application of the PDPA.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and comply with sector specific requirements. Organizations that outsource to third parties will be held liable together with the third party provider in case of breach by the latter.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

Under the PDPA, public institutions and non-public institutions have the obligation to notify the affected individuals by appropriate means in the event of a data security breach. Under the draft Enforcement Rules for the PDPA, the “appropriate means” shall mean any method which can deliver the message to the affected individuals, including written notice, telephone, facsimile, or electronic transmission. However, in the event that costs may be substantial, public notice is allowable. The notice should contain how the data security was breached and the remedy already adopted.

An organization that is involved in a data breach situation may be subject to closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions and/or class actions, or a criminal prosecution.
16. Accountability
There is no requirement under the PDPA for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of personal data.

17. Whistle-blower hotline
Taiwan does not have whistleblower legislation.

18. E-discovery
Taiwan does not have common law pre-trial discovery procedures (including e-discovery). There are requirements that evidence can be introduced at certain points during the trial process. However, an e-discovery system is not widely used. Therefore, it is prudent to obtain consent in advance or to specify in the employees handbook that the company may access Personal Data in the e-discovery process.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, it is advisable to provide in the employees handbook that company email accounts are for business purposes only and that the company may process or use the company email accounts for business related purposes, including implementation of a spam-filtering solution.

20. Cookies
There are no specific laws/rules that regulate the deployment of cookies in Taiwan.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.
Thailand

**Pattaraphan Paiboon**
Bangkok  
Tel: +66 02 636 2000 Ext. 4568  
pattaraphan.paiboon@bakermckenzie.com

**Dhiraphol Suwanprateep**
Bangkok  
Tel: +66 02 636 2000 Ext. 4950  
dhiraphol.suwanprateep@bakermckenzie.com
1. Recent Privacy Developments

The Personal Data Protection Bill was approved in principle by the Cabinet on 6 January 2015. The latest version of the bill was further revised as proposed by the Council of State in May 2015. Meanwhile, the Thai government has initiated a digital economy plan in order to promote IT business and the digital environment in Thailand. The Personal Data Protection Bill was included in the set of draft laws to promote the digital economy in Thailand. These draft laws under the digital economy plan have already been approved in principle by the Cabinet between December 2014 and January 2015. They are currently being considered by the Council of State. Please see a summary of the draft laws regarding digital economy below.

(1) The Digital Development for Economy and Society Bill. This is a combination of three bills which were proposed separately earlier, the Committee for Digital Economy and Society Bill, the Promotion of Digital Economy Bill, and the Digital Development Fund for Economy and Society Bill. The bill establishes the Committee for Digital Economy and Society, Digital Development Fund, and Digital Economy Promotion Office.

(2) The Ministry, Department, and Bureau Reform Bill. It is aimed at reforming the Ministry of Information and Communications Technology (MICT) into the Ministry of Digital Economy and Society to be the Ministry responsible for digital economy developments.

(3) The Draft Amendment to the Electronic Transactions Act. It revises criteria for conducting electronic transactions and revises the structure, power, and duties of the Electronic Transactions Commission.

(4) The Draft Amendment to Computer Crime Act. It revises criteria for computer crimes and the power of the relevant officials under the Bill.

(5) The National Cybersecurity Bill. It provides criteria for ensuring cyber security and establishes a National Cybersecurity Committee (NCSC).

(6) The Personal Data Protection Bill. It provides criteria for collecting, using, and disclosing personal data. It also provides the rights of data owners and establishes a Data Protection Committee.

(7) The Draft Amendment to the Organization to Assign Radio Frequencies and to Regulate Broadcasting and Telecommunications Businesses Act. It revises and supplements licensing criteria for allocation of radio frequencies. It also revises the power and duties of the National Broadcasting and Telecommunications Commission (NBTC).
(8) **The Draft Amendment to the Royal Decree Establishing the Electronic Transactions Development Agency (Public Organization).**

It revises and supplements the powers and duties of the Office of Electronic Transactions Development Agency (ETDA).

As Thailand does not yet have a consolidated data privacy law in general, the Personal Data Protection Bill would be the first general data protection law in Thailand. If the bill is passed according to the current unofficial draft bill, the data owners' consent is required before or at the moment of collection, use, and disclosure of personal data. Such bill is expected to be passed within the course of this year. After approval of from the Council of State, it will be forwarded to the Cabinet and later to the National Legislative Assembly (NLA) for further consideration. Once the NLA endorses the draft law, it will be sent to His Majesty the King for final approval before being published in the [Government Gazette](#).

2. Emerging Privacy Issues and Trends

*Mandatory Breach Notification*

Under the Telecommunications Business Act, if there is a breach of the telecommunications users’ rights in relation to personal information, privacy, or the right to communicate through telecommunications, telecommunications operators must notify affected users without delay. If the Personal Data Protection Bill is passed in its current form, there will be a requirement for breach notification. The personal data controller is required to notify the data owner of the breach and the cause of breach immediately, and also the remedial plan for damage caused by such breach. If the breach affects over the amount of people to be prescribed by the Data Protection Committee, the personal data controller must also report the breach to the Data Protection Committee.

*Anti-spam Legislation*

Currently, the Computer Crime Act B.E. 2550 (2007) prohibits anyone from committing any illegitimate act by blocking, slowing down, obstructing or interfering with the computer system of another person so that it can no longer perform its function properly. Therefore, anyone who sends repetitive and continuous emails to the extent of causing other person’s computer system to fail is subject to the act. Furthermore, the act also prohibits sending spam mail which conceals or falsifies its origin to others. Nonetheless, the Draft Amendment to the Computer Crime Act, if passed in the current form, prohibits anyone from sending computer data or email which will impair the peaceful use of others’ computer systems, without an option for receivers to opt out from such mailing.
Cloud computing

There is no specific legislation governing cloud computing at the moment. However, the Bank of Thailand issued a circular regulating the use of cloud computing by financial institutions.

Electronic Contracting

The Draft Amendment to the Electronic Transactions Act, if passed in the current form, specifically prescribes the validity or enforceability of a contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems.

Electronic Signatures

The Draft Amendment to the Electronic Transactions Act, if passed in the current form, will change the criteria of electronic signatures to be broader and focus on the intention of the electronic signature owner. This will be in line with the United Nations Convention on the Use of Electronic Communications in International Contracts.

Cybersecurity

The National Cybersecurity Bill will establish the NCSC as a central command center focusing on cyber terrorists and cyber attacks in Thailand and maintaining national security, military security, and economic stability in the cyber world. If the bill is passed in its current form, the NCSC will be in charge of preparing a master plan, guidelines, measures, operation plans, or projects related to cybersecurity. Therefore, any private entity may be required by the NCSC to act or not to act, and notify the NCSC if there is a cyber attack which may affect the financial stability, commerce, or national security.

3. Law Applicable

The rights to privacy have also long been recognized in the Thai legal system. As such, a person shall have the right to be accorded protection against undue exploitation of personal data relating to his or her individuality, as provided by law. In the absence of specific legislation on data privacy in Thailand, the most relevant law relating to data privacy available at the moment would be the law of wrongful act (tort).

Theoretically, any violation of the Constitution that results in damage to others may constitute a wrongful act (a tort) under the Thai Civil and Commercial Code (CCC). However, to date no court decision that interprets the provisions of the Constitution in this light has been issued.

In addition to the above, the use and/or transfer of certain types of personal data is subject to some prohibitions/controls, depending on the type of business sector involved. For example, the following legislation on data privacy:
4. Key Privacy Concepts

a. **Personal Data**

Under the Privacy Notification, “personal data” includes information such as a telecommunications user’s name; date of birth; or other facts and details relating to a user which may identify the user; telecommunications numbers; and how the user uses telecommunications services.

The Credit Bureau Act protects information in relation to customers who obtain credit such as: (i) the facts identifying the customers and the qualifications of such customers; and (ii) the records of applications, credit approval and credit payment of customers who apply for credit.

The Child Protection Act does not prescribe a specific definition of the information about a child or his or her parents. However, it generally protects the information of a child or his or her parents, e.g. their names, photographs, or any information in a way that may harm a child’s or parent’s reputation, honor, or benefits.

The Personal Data Protection Bill defines “personal data” as the data relevant to a person, which can identify the person directly or indirectly, excluding only names, titles, workplaces, or business addresses, and information on the deceased.

b. **Data Processing**

The Privacy Notification provides that data processing includes any action concerning usage, disclosure or amendment of the users’ personal data by any means, and includes the sending or transfer of personal data used in the telecommunications business operation.
Under the Credit Bureau Act, data processing includes any operation performed upon information, whether to collect and compile, record, arrange, store, amend, recover, use, disclose, print, access, delete, or destroy the information.

The Personal Data Protection Bill does not directly address the processing of the personal data.

c. Processing by Data Controllers

The Privacy Notification imposes duties and restrictions on a person or entity granted a license to operate a telecommunications business in Thailand by the NBTC.

The Credit Bureau Act imposes duties and restrictions on credit bureau company and their members. A credit bureau company is an operator of business concerning the control and/or processing of credit information for the purpose of giving credit information to members, or an entity which lawfully operates a business by providing credit in its normal course of business. Members are licensed to operate financial businesses in Thailand and are authorized by the credit bureau company.

The Child Protection Act applies to all persons and entities in Thailand.

The Personal Data Protection Bill imposes duties and restrictions on the data controller in the collection, use or disclosure of Personal Data.

d. Jurisdiction/Territoriality

While the Privacy Notification applies to licensees who operate telecommunications business in Thailand, the Credit Bureau Act applies to licensees authorized to operate a credit bureau company in Thailand.

The Child Protection Act, applies to the dissemination of information about children and/or their parents in Thailand.

The Personal Data Protection Bill will also apply to data controllers in Thailand.

e. Sensitive Personal Data

The Privacy Notification does not specifically identify the following information as being sensitive personal data, but it nonetheless prohibits the collection of the following information from users:

- physical disability, except for the collection of such data for the purpose of providing suitable services according to the disability;
- genetic descriptions; and
- data that may affect the feelings or which may cause damage, or may clearly compromise the freedom of the service user, as prescribed by the NBTC.
The Credit Bureau Act does not specifically identify the following information as being sensitive personal data, but it nonetheless prohibits the collection of information about the following:

- physical disability conditions;
- genetic data conditions;
- data of a person who is participating in an inquiry or criminal trial; and
- any other data that is not relevant to using the service, or applying for credit, or might cause damage, or impact the rights and freedoms of the data owner as will be announced by the Credit Information Committee.

The Personal Data Protection Bill also regulates data controllers from collecting certain data, unless the data owner’s consent is obtained, e.g., race, ethnicity, political opinions, religious beliefs, criminal history, medical history, etc.

f. Employee Personal Data

No specific requirements apply under the Privacy Notification, the Credit Bureau Act or the Personal Data Protection Bill.

5. Consent

a. General

The Privacy Notification regulates that consent of the data owner is required in order to process any personal data. The data processing must be carried out for the purpose of telecommunications business operation, and must comply with the Privacy Notification. There are certain instances, however, where consent is not required.

Furthermore, under the Personal Data Protection Bill, personal data cannot be collected, used, or disclosed unless consent is obtained from the data owner. There are some exemptions from such consent, e.g., for research or statistics, such personal data being kept confidential, etc.

b. Sensitive Data

There are no specific requirements on obtaining consent in relation to sensitive data under the Privacy Notification and the Credit Bureau Act.

According to the Personal Data Protection Bill, certain data, e.g., race, ethnicity, political opinion, religious beliefs, criminal history, and medical history, are deemed sensitive and cannot be collected without data owner’s consent as described in 4(e) above.

c. Minors

There are no specific requirements under the Privacy Notification, the Credit Bureau Act, the Child Protection Act or the Personal Data Protection Bill.
Generally, while consent cannot be obtained from minors, it can be given by a legal guardian or parent on behalf of the minor, or from the minor himself/herself depending on the circumstances.

d. Employee Consent
There are no specific requirements under the Privacy Notification, the Credit Bureau Act and the Personal Data Protection Bill.

e. Online/Electronic Consent
There are no specific requirements under the Privacy Notification and the Credit Bureau Act.

The Personal Data Protection Bill prescribes the form of consent to be in writing or given via an electronic system, unless consent cannot be obtained by such methods.

6. Notice Requirements
According to the Privacy Notification, a telecommunications licensee that collects personal data must provide data owners with information about, e.g. the period of data retention, user’s rights, the person to whom the personal data has been sent and how the personal data will be processed, criteria on personal data rights protection and privacy rights, and the right to file a complaint. The credit bureau company members must inform the clients regarding the information sent to the credit bureau company in writing.

According to the Personal Data Protection Bill, data controllers will be required to notify data owners before or at the moment of collecting personal data of certain details, e.g. the objectives of collection, types of persons or organizations that personal data might be disclosed to, rights of the data owner, etc.

7. Processing Rules
According to the Privacy Notification, a telecommunications licensee that processes personal data must carry out such processing for purpose of telecommunication business operation and must comply with the Privacy Notification. The Personal Data Protection Bill requires that data controllers must process the personal data according to the objectives informed to the data owner.

8. Rights of Individuals
According to the Privacy Notification, the users have the right to request or inspection, copy or certified copy of personal data, request for change or amendment of personal data, request for suspension of usage or disclosure of personal data, and withdraw the consent to process personal data at any time.
The Credit Bureau Act also gives the data owner right to know which of information is kept by the credit data company, right to check their data, right to object the incorrect data, etc.

Personal Data Protection Bill also sets out data owner rights, e.g., right to access the owner’s data, or right to access such data obtained without the owner’s consent.

9. Registration/Notification Requirements
Currently, there are no requirements for an organization that collects and processes personal data to register with the local data protection authority, or file with and notify the appropriate data protection authority.

10. Data Protection Officers
According to the Personal Data Protection Bill, the Personal Data Protection Committee will be set up to be in charge of personal data.

11. International Data Transfers
The Privacy Notification requires that telecommunications licensees must obtain consent from data owners before international data transfers and it must be for telecommunications business purpose.

The Credit Bureau Act prohibits the control or processing of data outside Thailand. Under the Credit Bureau Act, the term “data” covers anything that conveys data relating to credit information or rating, irrespective of the form. The Personal Data Protection Bill requires that the transfer of personal data to other countries must comply with a sub-regulation to be issued by the Data Privacy Committee, with certain exceptions.

12. Security Requirements
The telecommunications licensee must set up measures for the prevention and protection of personal data both in terms of technical aspects and internal management, e.g., changing the access and deciphering systems used for the protection of personal data at least every three months. According to the guideline provide by the Credit Information Protection Committee, organizations are required to take steps to ensure that personal data in its possession and control are protected from unauthorized access and use, implement appropriate physical, technical and organization security safeguards to protect personal data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the personal data involved. The Personal Data Protection Bill also regulates the data controllers’ obligations, for example, the data controllers must provide security methods to prevent loss, access, use, change, alteration, or disclosure of personal data without the authority to do so, etc.
13. Special Rules for Outsourcing of Data Processing to Third Parties

The Privacy Notification requires the telecommunications licensee to provide: the details and impose obligations/liabilities of the person assigned to undertake the processing of personal data or compilation of user directories and personal information.

The Credit Bureau Act requires persons entrusted to conduct data processing to implement certain systems and comply with certain requirements in processing personal data.

Under the Personal Data Protection Bill, if personal data is granted to third parties, data controllers must take measures to prevent third parties from using or disclosing personal data without authority.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data protection authority investigations or audits, data protection authority orders, administrative fines, penalties or sanctions, civil actions, criminal penalties, and private rights of action.

15. Data Security Breach

No specific requirements apply under the Privacy Notification, Child Protection Act, and Personal Data Protection Bill. Nevertheless, the Credit Information Protection Committee issued a guideline on the security of credit information services, providing that a credit bureau company for which the data security have been breached must promptly inform staff, media, members and users of the problem and the proposed solution. Furthermore, a report made in writing on the security breach must be provided to the board of directors of the credit bureau company. The report should include:

- the date, time and place where data security was breached;
- the characteristics and method used to breach the data security and the offender (if known);
- the cause and damages incurred by indicating the specific data and/or the system damaged;
- the evaluation of the damages occurred; and
- measures taken to tackle the problem and further measures to be implemented.
16. Accountability
There is currently no specific requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of personal data.

17. Whistle-blower hotline
There are no specific laws/rules in Thailand that govern the establishment of a whistle-blower hotline.

18. E-discovery
Not applicable, as Thailand currently does not have an e-discovery system.

19. Anti-Spam Filtering
There are no specific laws or regulations restricting the installation of spam-filtering within organizations in Thailand. Nonetheless, the Telecommunications Business Act prohibits intercepting, making use of, or disclosing data information or other information communicated through telecommunications without authorization.

20. Cookies
There are no specific laws or rules in Thailand that regulate the use and deployment of cookies.

21. Direct Marketing
According to the Direct Sales and Direct Marketing Act, B.E. 2545 (2002) (Direct Sales Act), “direct marketing” means the marketing of goods and services by way of communicating information in order to offer to sell goods or services directly to consumers at a distance and with the anticipation that individual consumers will respond and purchase the goods or services from the direct marketing operator.

Under the Direct Sales Act, business operators wishing to conduct direct sales or direct marketing business will be required to obtain a direct marketing license under the Direct Sales Act prior to the commencement of such business.
Turkey

Hakki Can Yildiz
Istanbul
Tel: +90 212 376 64 54
can.yildiz@bakermckenzie.com

Can Sozer
Istanbul
Tel: +90 212 376 64 43
can.sozer@bakermckenzie.com
1. Recent Privacy Developments

Draft Code on the Protection of Personal Data

The 2008 Draft Code on the Protection of Personal Data (the “Draft Code”), updated in December 2014, which aims to harmonize Turkish data protection law with the Council of Europe’s Convention (No. 108/1981) for the Protection of Individuals with Regard to Automatic Processing of the Personal Data (the “European Data Protection Convention”) and the EU Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (the “EU Directive”), has not yet been enacted. While the Draft Code has not yet been adopted, parliamentary commissions are in the process of finalizing it. In January 2015, the Draft Code was referred to the Justice Commission, the last stop before parliamentary discussions. The discussions on the Draft Code will resume in September 2015 when the Parliament will convene for the first time after the June 2015 elections. Still, the fact that the Draft Code has already been submitted to the Parliament is a long-awaited, significant step in Turkey’s progress toward adopting a privacy law.

2. Emerging Privacy Issues and Trends

On October 23, the Turkish parliament adopted the long-awaited Law on Regulation of Electronic Commerce (the “E-Commerce Law”). Among many other new rules, the E-Commerce Law bans commercial messages by email, text messaging (sms), fax, and autodial machines (robocalls) to consumers without their prior approval. The e-commerce service providers will be responsible for storing and securing the personal data obtained from the online agreement. The service provider will not be able to transfer the personal data to third parties without the buyer’s consent, or use the data for other purposes. Please refer to Section 21 on Direct Marketing for further information.

3. Law Applicable

Turkey does not have a specific data protection law. The Turkish Constitution as well as certain Turkish laws, however, contain provisions on data protection – such as the Civil Code, Code of Obligations, Labor Law, Criminal Code, Banking Law, Health and Medicine Law and Electronic Communication Law.

Turkey has signed the European Data Protection Convention, but has not ratified it. This Convention contains a broad definition of “Personal Data”, which means any information relating to an identified or identifiable individual (the “Data Subject”). Although Turkey has not yet ratified the Convention, its definitions are relied upon in practice.
In light of amendments to the Turkish Constitution in 2010, protection of Personal Data is deemed an individual right, and as a result, the recording, processing or transfer of Personal Data are restricted. According to Article 20 of the Constitution, personal data can only be processed if required by law or upon the data subject’s explicit consent. Processing, including transfer, of personal data without the consent of the data subject may lead to violation of the personal rights, result in indemnities and other legal remedies. To this end, explicit consent must be obtained to ensure compliance with the legislation, and such consent must comply with morality and the laws.

The following are important privacy provisions under Turkish law:

**Turkish Constitution.** In addition to Article 20 above, Article 17(I) of the Constitution provides that “every individual is entitled to rights of living, protection and improvement of his material and spiritual being.”

**Turkish Civil Code.** Articles 23, 24 and 25 of the Turkish Civil Code safeguard personal rights. Article 23 sets out that “no individual may waive his/her freedom or restrict his/her freedom contrary to morality and law”. Furthermore, Article 24 provides legal remedies, stating that “violation of personal rights is unlawful unless justified by the consent of the person whose rights have been violated, superior private or public benefit, or authority granted by law”. Article 25 also sets out certain civil remedies in case of infringement of personal rights.

**Turkish Code of Obligations.** Pursuant to Article 27 of the Turkish Code of Obligations, an agreement contrary to personal rights is invalid. Furthermore, under Article 58, a person whose personal rights have been violated may seek damages against the person who has violated those rights. Additionally, Article 419 imposes a duty on an employer in relation to employee Personal Data. Pursuant to this provision, an employer may only use employee Personal Information where it is related to the employee’s qualifications or if it is required to perform a service.

**The Turkish Labor Law.** Article 75 of the Turkish Labor Law states that “the employer shall arrange a personnel file for each employee working in its establishment. In addition to the information about the employee’s identity, the employer is obligated to keep all the documents and records in its possession in accordance with this Act and other legislation and to show them to authorized persons and authorities when requested. The employer is obligated to use information obtained about the employee consistent with the principles of honesty and law and not to disclose information which the employee has a justifiable interest in keeping secret”.

In Turkey, employers generally receive the following from employees: employee application forms, copies of identification cards, certificates of residence, copies of diplomas, certificates of proficiency (if any), employment contracts, health reports, original disability reports (for disabled employees),
warning letters regarding employment health and security, and conviction records. To the extent that Article 75 is applicable, the employers are only permitted to use such data according to this provision.

Under certain circumstances, an employee may terminate his or her employment contract for cause under the Labor Law in the event of an invasion of privacy.

**Turkish Criminal Code.** Personal Data and privacy are also safeguarded under the Turkish Criminal Code. For instance, under Article 134 of this Code, a person who violates the secrecy of a person’s private life may be fined or imprisoned for one to three years. According to Article 135 of the Turkish Criminal Code, illegally recording Personal Data, violating the data recording prohibition or data recording without consent of the relevant person, and illegally recording data relating to the political, philosophical, or religious views, or ethnic origins of individuals or moral inclinations, sex lives, health conditions or union affiliations may subject the offender to six months to three years imprisonment. Similarly, under Article 136 of this Code, the illegal transfer, dissemination and collection of Personal Data is punishable by imprisonment of one to four years.

Pursuant to Article 138 of the Turkish Criminal Code, if a person whose responsibility is to delete Personal Data at the end of the retention period fails to do so, that person may be imprisoned for six months to one year. Nevertheless, the sanction of imprisonment only applies to natural persons; the Turkish Criminal Code also sets forth security measures applicable to legal entities.

**Electronic Communications Act.** Article 51 of the Electronic Communications Act contains detailed rules on the protection and management of personal data in the electronic communications sector. These rules include, but are not limited to, the new rule allowing international transfer of personal data with explicit consent. According to Article 51, personal data may only be processed when explicitly permitted by law and in line with principles of good faith. Additionally, electronic communications and traffic data are deemed private; therefore, the recording, retention, interception or tracking of electronic communications, in the absence of another legal basis or the consent of the data subject (i.e., parties to the communication), is prohibited. Moreover, retaining and accessing data in users’ terminal equipment for purposes other than those related to the provision of electronic communications services, are permitted only after obtaining the users’ informed consent. Electronic communications operators are obligated to take administrative and technical measures to ensure the security of their users’ personal data.
4. Key Privacy Concepts

a. Personal Data
In addition to some definitions provided in specific Turkish regulations, the definition of Personal Data in the European Data Protection Convention is relied upon in practice in Turkey – Personal Data means any information relating to an identified or identifiable individual Data Subject. As a consequence, Personal Data includes information on a person’s identification number; physical, psychological, mental, health, genetic or economic condition; cultural or social identity; ethnicity; religion; family; and political affiliations.

b. Data Processing
In addition to some definitions provided under specific regulations under Turkish law, the definition of automatic processing in the European Data Protection Convention is relied upon in Turkish practice. “Automatic processing” includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.

c. Processing by Data Controllers
Turkish law does not expressly regulate data processing by Data Controllers. The Draft Code, however, distinguishes between data controller and data processor concepts in line with the EU Directive. That said, unlike the EU Directive, data controller is defined in the current text of the Draft Code as a “Real or legal person responsible for the establishment and management of data registration system”.

d. Jurisdiction/Territoriality
Article 35 of the Law on International Private Law and Procedure Law No. 5718 provides that “claims arising from the violation of personal rights through the media such as radio, press, television, the Internet or any other mass media will be governed by, at the discretion of the aggrieved party (i) the law of the aggrieved party's habitual residence, provided the injurer is in a position to be aware that damage could occur in that jurisdiction, (ii) the law of the injurer’s place of business or habitual residence, (iii) the law of the jurisdiction where the damage occurred, provided that the injurer is in a position to be aware that the damage could occur in that jurisdiction”. It further sets forth that “[t]he first clause of this article is also applicable to claims arising from violation of personal rights by processing Personal Data or restricting right to demand information regarding Personal Data”.
e. **Sensitive Personal Data**

Turkish law does not specifically recognize Sensitive Personal Data as a separate category of data. However, the types of Personal Data specified under Article 135 of the Turkish Criminal Code, in particular, Personal Data relating to political, philosophical or religious views, or ethnic origins of individuals or moral inclinations, sex lives, health conditions or union affiliations, could be deemed Sensitive Personal Data.

f. **Employee Personal Data**

Turkish law does not separately address employee Personal Data. If it is deemed personal data, the abovementioned legal framework applies.

5. **Consent**

a. **General**

Explicit consent of the Data Subject is required prior to the collection, processing and disclosure of Personal Data. Explicit consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances.

The appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to only cover the identified purposes. Fresh consent is required for purposes that have not been previously identified and consented to.

The Data Subject also has the right to withdraw consent at any time in given circumstances.

Consent does not need to be in the local language, but the Data Subject must understand the language in which consent is given.

b. **Sensitive Data**

Turkish law does not specifically recognize Sensitive Personal Data as a separate category of data. If data is deemed Personal Data, the abovementioned legal framework applies.

c. **Minors**

A parent of a minor may consent on behalf of the minor. Unless the minor is deemed to have reached legal age pursuant to a court decision or by marriage, the legal age for Turkish citizens is 18 years. Depending on the type of data, a minor may need to renew his or her consent upon reaching legal age. In any event, a minor may withdraw the consent upon reaching the age of majority.
d. Employee Consent

Article 75 of the Turkish Labor Law states, “[t]he employer shall arrange a personnel file for each employee working in its establishment. In addition to the information about the employee’s identity, the employer is obligated to keep all the documents and records in its possession in accordance with this Act and other legislation and to show them to authorized persons and authorities when requested. The employer is obligated to use information obtained about the employee consistent with the principles of honesty and law and not to disclose information which the employee has a justifiable interest in keeping secret”.

In Turkey, employers generally receive the following from employees: employee application forms, copies of identification cards, certificates of residence, copies of diplomas, certificates of proficiency (if any), employment contracts, health reports, original disability reports (for disabled employees), warning letters regarding employment health and security, and conviction records. To the extent that Article 75 is applicable, employers are only permitted to use such data in accordance with this provision.

Additionally, Article 419 of the new Code of Obligations imposes a duty on an employer in relation to employee Personal Data. Pursuant to this provision, an employer may only use employee Personal Information where it is related to the employee’s qualifications or if it is required to perform a service.

The Turkish Appellate Court, however, ruled that “an employer is entitled to monitor, at any time, the computer and email addresses owned by the employer and emails received in such email addresses.” Thus, an employer is entitled to review the office emails of its employees. An employer, however, cannot review an employee’s private emails.

e. Online/Electronic Consent

Electronic consent is permissible and enforceable in Turkey provided that it is properly structured and evidenced.

6. Information/Notice Requirements

There are no current rules under Turkish law on information/notice requirements. Based on the Draft Code and best practices, organizations that collect Personal Data must provide Data Subjects with information about the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to contact the privacy officer or other person who is accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; how to access and/or correct the Data Subject’s Personal Data; the
duration of the proposed processing; and the means of transmission of the Personal Data.

7. Processing Rules
There are no current rules under Turkish law on processing rules. Based on the Draft Code and best practices, organizations that process Personal Data limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; anonymize the Personal Data whenever possible; provide the Data Subject the option to use a pseudonym or remain anonymous whenever possible; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. Registration/Notification Requirements
There are currently no requirements for organizations that collect and process Personal Data to register, file or notify the local data authority. If and when the Draft Code is enacted, organizations that collect and process Personal Data will have to register with the local data protection authority, which will be established in accordance with the Draft Code.

10. Data Protection Officers
There is no requirement for organizations to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers
Except for data obtained through electronic communications, Turkish law does not specifically regulate data transfers abroad. As mentioned above, the only rule which permits transfer of personal data abroad upon obtaining the users’ consent is the sector-specific Article 51 of the Electronic Communications Act. However, even in the absence of an umbrella law or other sector-specific legislation, the notice and consent requirements apply to international transfers of data.
Organizations may transfer Personal Data outside of Turkey provided that impacted Data Subjects have been informed or have provided consent; and that reasonable steps have been taken to safeguard the Personal Data to be transferred.

12. Security Requirements

There are no current rules under Turkish law on security requirements. Based on the Draft Code and best practices, organizations take appropriate measures to ensure that Personal Data in their possession and control is protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved. If an organization causes any security breach and such breach gives harm to the Data Subject, or any party that the organizations is in a contractual relationship with, these persons may claim damages based on the general principles of Turkish law, e.g., the Civil Code. That is why it is advised that the organizations take appropriate security measures to mitigate this risk.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and are required to comply with sector specific requirements. Organizations may be held liable together with third party providers in case of breach by the latter.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, administrative fines, penalties or sanctions, civil actions, criminal proceedings, and/or private rights of action.

15. Data Security Breach

There are no specific rules addressing data security breaches. Pursuant to general principles of law, persons at risk of suffering damage due to a data security breach must be notified of the breach and information compromised. Additionally, if the data security breach constitutes a crime, judicial authorities (including the prosecutor’s office or the police) must be informed of the breach pursuant to Article 278 of the Criminal Code.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, civil actions, class actions, or a criminal prosecution.
16. Accountability
Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
There is no specific law/rule that governs whistle-blower hotlines in Turkey.

18. E-Discovery
When implementing an e-discovery system, an organization may be required to obtain the consent of employees if the collection of Personal Data is involved, and advise employees of the implementation of the system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.

20. Cookies
There are no specific laws/rules in Turkey that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Consent of Data Subjects may have to be obtained before cookies can be used.

21. Direct Marketing
On October 23, the Turkish parliament adopted the long-awaited Law on Regulation of Electronic Commerce (the “E-Commerce Law”). Among many other new rules, the E-Commerce Law bans commercial messages by email, text messaging (sms), fax, and autodial machines (robocalls) to consumers without their prior approval. Previously, it was permitted to send unsolicited messages if consumers were provided an easy and free-of-charge opportunity to opt-out. Under the E-Commerce Law, commercial messages can be sent to a consumer electronically only if the consumer has given prior approval. Approval must be obtained either electronically or in writing.

The content of the commercial message must be in line with the approval given. The message also must include (i) sender identity; (ii) sender phone number/fax number/sms number/email, depending on the electronic means used; (iii) subject and purpose of the message; and (iv) information on the actual sender, if the message is sent on behalf of another entity.
As consumers always have the right to opt-out of receiving commercial messages, the sender must provide them an easy and free-of-charge opportunity to revoke their prior approval; details of this opportunity must be contained in the message.

The opt-in system will not apply to B2B relationships and commercial messages can still be sent to businesses without their prior approval.

The service provider will be responsible for storing and securing the personal data obtained from the online agreement. The service provider will not be able to transfer the personal data to third parties without the buyer's consent, or use the data for other purposes.

The law entered into force on 1 May 2015.
Ukraine

Oleksiy Stolyarenko
Kyiv
Tel: + 380 44 590 0101
oleksiy.stolyarenko@bakermckenzie.com
1. Recent Privacy Developments

Reforming the administration of Personal Data Protection

In July 2013, the Ukrainian Government adopted a draft law that introduced amendments to the Personal Data Protection Law in Ukraine. As a result, all Personal Data protection functions were transferred from the State Service of Personal Data Protection to the Ukrainian Parliament Commissioner for Human Rights (“Commissioner”) effective 1 January 2014.

As such, the Commissioner was tasked to develop all Personal Data protection procedures, recommendations and enforcement practices that regulate matters related to Personal Data protection. To date, the Commissioner has drafted and approved: Model Rules on Personal Data Processing; Rules on Exercising Control by the Ukrainian Parliament Commissioner for Human Rights over compliance with laws on Personal Data protection; Rules for Notification of the Ukrainian Parliament Commissioner for Human Rights on Processing of Personal Data that Constitutes Special Risk for Rights and Freedoms of Data Subjects, On Structural Department or Designated Individual Responsible for Work-Related Processing of Personal Data and the Publication of Such Information.

The transition has resulted to the absence of enforcement actions related to Personal Data regulations in Ukraine from approximately January 2014 up to August 2015. However, this trend may change beginning August 2015 as most of the basic procedures and regulations necessary for enforcement have already been developed and approved by the Commissioner.

In addition, registration of databases containing Personal Data is no longer mandated; instead, Data Controllers are required to notify the Commissioner of the processing of certain types of sensitive information.

2. Emerging Privacy Issues and Trends

Two draft laws currently registered at the Ukrainian Parliament relate to Personal Data protection in conjunction with the ongoing antiterrorist operations in Ukraine.

The first draft law, No. 2959 dated 26.05.2015, proposes to allow Personal Data processing for legal entities and individuals in order to assist the Ministry of Internal Affairs of Ukraine, the General Prosecutor of Ukraine, the Ministry of Defense of Ukraine, the State Border Guard Service of Ukraine, the Security Service of Ukraine, the Foreign Intelligence Service of Ukraine in the implementation of the necessary measures to protect people and public safety against crimes associated with antiterrorist operations in Ukraine.

The second draft law, No. 2043а dated 08.06.2015, proposes to introduce liability of military personnel for offenses related to Personal Data protection. In addition, this draft law improves and strengthens administrative liability for
non-compliance with demands of the Commissioner for all Personal Data offenses.

3. Law Applicable

The Law of Ukraine On Personal Data Protection adopted in 2010 ("PDP")\(^1\) outlines the general requirements and obligations related to the collection, processing and use of Personal Data by private bodies and by the government of Ukraine.

Under the PDP, processing of Personal Data is not restricted under the following circumstances (i) individuals processing of Personal Data for their own personal or domestic activities, (ii) processing of Personal Data solely for journalistic and artistic purposes, provided that the balance between the right to respect for private life and the right to freedom of expression are secured. In addition, the PDP does not apply to archived information from repressive totalitarian organizations within the territory of Ukraine from the period 1917-1991.

In addition, the main sources of Personal Data protection in Ukraine are: The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional Protocol ratified by Ukraine in 2010; a number of regulations approved by the Commissioner; and respective provisions of the Code of Ukraine on Administrative Offenses; and the Criminal Code establishing respective liability for Personal Data offenses.

4. Key Privacy Concepts

a. Personal Data

The PDP applies to the “processing” of “Personal Data,” i.e., any information about an individual who is identified or can be specifically identified ("Data Subject").

The Constitutional court of Ukraine, in its decision N 2-rp/2012 dated January 20, 2012, held that “Personal Data” constitutes confidential personal information access to which is limited by a person himself/herself. Such confidential personal information may include the data about the individual’s nationality, education, marital status, religious beliefs, health, current address, date and place of birth, and property status. The list of confidential personal information is not exhaustive.

b. Data Processing

“Processing of personal data” - any action performed manually or through the means of automated systems including but not limited to acquisition, registration, accumulation, storage, adaptation, modification, restoration, use

\(^1\) [http://zakon4.rada.gov.ua/laws/show/2297-17/print1433741768298759](http://zakon4.rada.gov.ua/laws/show/2297-17/print1433741768298759)
and distribution (dissemination, sale, transfer), depersonalization and destruction of Personal Data.

c. **Processing by Data Controllers**
The PDP applies to any person or legal entity which processes Personal Data on his, her or its own behalf ("Data Controller").

"Data Controller" is defined by the PDP as a person or a legal entity that establishes the purpose of processing Personal Data, and sets the scope and procedures of the data processing.

d. **Jurisdiction/Territoriality**
The PDP applies to all Personal Data processing (i.e., to acquisition, registration, accumulation, storage, adaptation, modification, restoration, use and distribution (dissemination, sale, transfer), depersonalization and destruction) within the territory of Ukraine. However, enforcement of the PDP against legal entities and individuals without legal presence in Ukraine is not established at the moment.

e. **Sensitive Personal Data**
Ukrainian data protection law recognizes the concept of sensitive data (direct translation: "special categories of Personal Data that constitute special risks to rights and freedoms of Data Subjects"). Data protection rules for sensitive data are more stringent.

Sensitive Data includes Personal Data on: racial or ethnic origin, national origin, political, religious or philosophical beliefs, membership in political parties and or organizations, trade unions, religious organizations or community organizations with ideological orientation, health, sex life, biometric data, genetic data, location and or ways of transportation, facts related to administrative or criminal liability, criminal investigation measures related to a preliminary investigation and the measures envisaged by the Law of Ukraine “On investigating activity”, and instances of violence against a person.

The PDP prohibits processing of Sensitive Personal Data unless certain conditions are met, including:

- a valid express consent obtained by the Data Collector from the Data Subject;
- an employer-employee relationship between the Data Collector and Data Subject;
- the data processing is necessary for protection of human life of the Data Subject or of a third party where the Data Subject is physically or legally incapable of giving consent;
- the data has evidently been made public by the Data Subject;
• the data is necessary to assert, exercise or defend legal claims;
• the data is processed by a religious organization, NGO, political party or trade union with respect to their members in the course of regular activities and such data would not be transferred to third parties;
• the data processing is necessary to establish medical diagnosis, to provide healthcare services or medical treatment, under condition that the data processed is protected by the medical confidentiality rules;
• the data processing conducted by law enforcement agencies and is related to criminal convictions, criminal investigations or counterterrorism activities.

The PDP requires from legal entities and individuals processing Sensitive Data to file respective notification to the Commissioner and appoint a Personal Data officer or establish a specific division responsible for Personal Data Protection.

f. Employee Personal Data

The PDP does not provide special rules for Employee Personal Data processing, therefore Employee Personal Data shall be processed on a general basis upon obtaining consent from the Employee.

5. Consent

a. General

Consent is an appropriate way to justify the collection, processing and use (including transfer) of Personal Data.

The Ukrainian Personal Data regulations define consent as the “voluntary act of the individual (duly informed) to permit the processing of Personal Data in accordance with the objectives set out for processing expressed in written or electronic form.”

Informed consent is understood to constitute “voluntary, competent decision of a person on the processing of his/her Personal Data that is based on receipt by this person in an objective manner and with full information with respect to future Personal Data processing.”

In order to make a voluntary and informed decision, a person, according to the Ukrainian Personal Data protection regulations, should be provided with responses on the following questions:

• Who will process his/her Personal Data? (Name of the processor of personal data, address, contact numbers, etc.)
• For what purpose will Personal Data be processed? (The goal of processing must be formulated clearly.)
• What Personal Data will be processed? (Specific exhaustive list of Personal Data to be processed)

• What specific actions will be performed on the Personal Data? (Collection, storage, transmission, publication, depersonalization, etc.)

• Who is the controller of the Personal Data? What are rights and obligations of the controller of personal data?

• To whom and where will Personal Data be transferred? For what purpose? On what grounds?

• How long will Personal Data be stored by the controller?

• Under what conditions can a person withdraw consent to the processing of Personal Data and the consequences of such action?

The Data Subject has a right to revoke his consent at any time. After revocation, the Data Controller and Data Processor must suspend the processing of Personal Data and destroy all of the Personal Data related to such Data Subject.

b. Sensitive Data

Ukrainian law recognizes Sensitive Data as a special category of Personal Data. It may be collected and processed with the express consent of the Data Subject, however, in certain prescribed circumstances, Sensitive Data may be processed without obtaining such consent.

c. Minors

The PDP does not provide clear guidance on the age requirements for minors to be legally capable to consent to Personal Data processing.

The Civil Code of Ukraine stipulates that minors from the age of 14 are capable to conclude small value contracts that correspond to the minors’ moral, social and physical level; can manage their own independent income, IP rights; have a right to become a shareholder/founder of a legal entity; open a bank account. All other legally binding actions by minors shall be approved by the parents or guardians.

Whether the minors can consent, and the extent of such consent to the processing of their Personal Data still remains to be decided by the Ukrainian authorities.

d. Employee Consent

The PDP does not stipulate any special rules applicable to obtaining Employee consent by the Employer, and, therefore, regular rules apply.
e. **Online/Electronic Consent**

Consent may be given in writing, i.e., ink signature and electronically, or it could also be included as one of the conditions of the contract, or consent could be provided in any other form, that leads to the conclusion that the consent has been provided (written application, questionnaire etc.), however, it is important to ensure that:

- the Data Subject has consented deliberately and unequivocally,
- consent is properly recorded and documented (for this purpose, the Data Subject should have to engage in any traceable activity, such as checking a box and then pressing a button),
- the Data Subject can access the consent wording at any time, and
- the Data Subject must be able to withdraw consent at any time with effect for the future.

6. **Information/Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; rights of Data Subject; and where the Personal Data is to be transferred.

7. **Processing Rules**

An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected and to period necessary to fulfil said purpose(s), but no longer than the period prescribed by the archive legislation or bookkeeping. In case, during processing it became evident that Personal Data contains incorrect information, such data should be amended immediately or destroyed.

The Data Controller need to obtain new consent from Data Subject if the identified purpose of the Personal Data processing has changed based on new identified purpose and scope.

8. **Rights of Individuals**

Data Subjects have a number of rights in Ukraine, including to be informed on sources of Personal Data collection, the location of their Personal Data, the purpose of processing, location of Data Controller. In addition, Data Subjects have a right to access their Personal Data, request modification of their Personal Data, in case it is outdated or elimination, in case, such data has
been collected illegally. Data Subjects can apply for protection from illegal Personal Data processing to the Commissioner, police or to the courts.

9. Registration/Notification Requirements

Any person or organization that processes Sensitive Personal Data is required by the PDP to send a proper notification to the Commissioner, which should include the following information:

- Types of Personal Data processed;
- Purpose of Personal Data processing;
- Category or categories of Data Subjects whose Personal Data is processed;
- Identities of third-party recipients of Personal Data;
- Cross-border transfers of Personal Data;
- Place (actual address) of data processing;
- General description of the technical and organizational measures taken by the Data Controller of Personal Data, to ensure its protection.

The PDP provides exceptions to the above requirement. As such, notification is not necessary in the following cases:

- Sensitive Personal Data is processed in order to be included into a database or registry that is open to the general public;
- Sensitive Personal Data is processed by public associations, political parties and/or organizations, trade unions, employers’ associations, religious organizations, NGOs with ideological orientation, provided that the processing of Personal Data relates exclusively to members of these associations and not transferred without their consent;
- Sensitive Personal Data is processed within the employee-employer relationship.

10. Data Protection Officers

The PDP requires legal entities and individuals processing Sensitive Personal Data to appoint an individual or establish a separate division responsible for Personal Data Protection.

The Data Officer/Designated Unit is responsible for consultations with the Data Controller/Processor on matters relating to compliance with Personal Data protection legislation and for the interactions with the Commissioner on matters related to the prevention and elimination of data protection violations. The Data Officer/Designated Unit oversees compliance with rights of Data Subjects with respect to Personal Data, analysis of security threats, and will
have access to all facilities and computer systems where Personal Data is processed. Upon identification of a Personal Data violation, the Data Officer/Designated Unit must report the matter to the Data Controller/Processor.

11. International Data Transfers

International transfers of Personal Data are allowed from Ukraine in the following cases:

- unequivocal consent for international transfer obtained from the Data Subject;
- the need to conclude or perform the transaction between the Controller of Personal Data and a third party - the subject of Personal Data for the benefit of Data Subject;
- the need to protect the vital interests of Data Subjects;
- the need to protect the public interest, to establish, secure and enforce legal demands;
- the Controller of Personal Data provided appropriate safeguards for non-interference in private and family life of the Data Subject.

Under the PDP, international data transfers are allowed to counties that provide adequate state protection of Personal Data. Under the PDP, country members of the EU/EEA and countries that ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data are considered as countries that provide adequate state protection of Personal Data. But Personal Data shall not be transferred and shared internationally for any other purpose than that for which it was collected.

12. Security Requirements

Personal data must be processed in a manner that prevents unauthorized access. The Data Controller/Processor independently designs special technical protection measures, including the exclusion of unauthorized access to Personal Data processed and of technical and software system, through which any access to Personal Data is controlled, logged and secured.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

Transfer of Personal Data from the Data Controller to the Data Processor is allowed only on the basis of an agreement in writing where parties agree on the scope, purpose of Personal Data processing and other respective security measures.
14. Enforcement and Sanctions
The requirements of the PDP are enforced in Ukraine by the Commissioner, police and courts, through the respective administrative, criminal and civil actions, which may result in administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
Ukrainian privacy regulations do not contain any specific rules related to Data Security breaches, therefore, the Data Controllers/Processors as well as infringers may be found liable for violation of the PDP on a general basis.

16. Accountability
Ukrainian privacy regulations do not contain any specific rules related to privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
Whistle-blower hotlines may be established in Ukraine provided that they are in compliance with local laws. There is no specific regulation from the Personal Data protection standpoint, however, all collection of Personal Data through such hotlines should comply with the PDP and respective rules.

18. E-Discovery
Ukrainian privacy regulations do not contain any specific rules related to E-Discovery systems, therefore, general provisions of the privacy law/regulations should apply.

19. Anti-Spam Filtering
Ukrainian privacy regulations do not contain any specific rules related to Anti-Spam Filtering, therefore, general provisions of the privacy law/regulations should apply.

20. Cookies
There are no specific laws/rules that regulate the deployment of cookies; hence, the general Ukrainian laws apply.

21. Direct Marketing
Direct Marketing activities require prior (opt-in) consent from the Data Subject who must have opportunity to unsubscribe from Direct Marketing (opt-out) anytime.
United Kingdom

Robbie Downing
London
Tel: +44 20 7919 1161
robbie.downing@bakermckenzie.com

Benjamin Slinn
London
Tel: +44 20 7919 1783
benjamin.slinn@bakermckenzie.com
1. Recent Privacy Developments

*Removal of requirement for the Information Commissioner’s Office (“ICO”) to establish that breaches of direct marketing rules amount to substantial damage and distress in order to impose monetary penalties*

From 6 April 2015, the ICO has the power to impose monetary penalties for serious breaches of the electronic direct marketing rules set out in the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the “E-Privacy Regulations”) without needing to be satisfied that such breaches were likely to cause substantial damage or distress. This amendment to the E-Privacy Regulations was made following a case in October 2013 where the First-tier Tribunal overturned a fine of £300,000 issued to an individual in relation to the sending of unwanted text messages in breach of the E-Privacy Regulations. This fine was overturned on the basis that the breaches concerned did not amount to “substantial damage and distress”, and this decision was upheld on appeal. The change to the E-Privacy Regulations will in practice make it easier for the ICO to impose monetary penalties for breaches of the electronic direct marketing rules under the E-Privacy Regulations, and the ICO’s current focus on enforcement in this areas is in relation to nuisance calls and text messages.

*ICO publishes paper on Big Data and Data Protection*

In July 2014 the ICO published a paper on big data and data protection which sets out the data protection issues arising out of big data and suggestions on how to comply with the Data Protection Act 1998 (“DP Act”). The ICO emphasises the importance of transparency in relation to big data and that the complexity of data analytics is not an excuse for organisations failing to obtain consent where it is required. The paper considers a number of data protection issues in relation to big data, including fairness, conditions for processing, repurposing data, data minimisation, subject access rights and security. The paper also provides suggestions for practical tools to assist with compliance in relation to big data, such as privacy impact assessments, privacy by design (including access controls, audit logs, data segregation and purpose limitation and separation) and transparency. The ICO states in the paper that it does not accept the argument that the data protection principles set out in the DP Act are not fit for purpose in relation to big data. The ICO states in the paper that the data protection principles should not be seen as barrier to progress, but a framework to promote privacy rights.

*Change to rules for Compensation under the Data Protection Act*

Under Section 13 of the DP Act, individuals can bring claims for compensation against a Data Controller if the Data Controller is in breach of the DP Act and the individual suffers damage (Section 13(1)). In addition, until recently an individual could claim compensation under Section 13(2) of the DP Act if they suffer distress by reason of a breach of the DP Act by the Data Controller only
if the individual has suffered damage or the breach relates to processing of personal data for special purposes (journalism, artistic or literary purposes). In the past this has been interpreted by the courts to mean that in order to successfully obtain damages for distress due to a breach by the Data Controller of the DP Act, the individual would need to have suffered pecuniary loss.

However, in a recent case the Court of Appeal held that it was arguable that Section 13(2) of the DP Act was ineffective, on the basis that it does not effectively transpose Article 23 of the Data Protection Directive (95/46/EC) which requires member states to provide that any person who suffers damage as a result of unlawful processing or any act which is in breach of national laws which implement the Data Protection Directive is entitled to receive compensation from the Data Controller for the damage suffered. In addition, the Court of Appeal held that it was arguable that Section 13(2) of the DP Act conflicts with Article 47 of the EU Charter on Fundamental Rights, which requires member states to provide that individuals have an effective remedy in relation to violations of the rights and freedoms set out in the EU Charter on Fundamental Rights, for example Article 7 (right to respect of private life) and 8 (right to protection of personal data). This case is under appeal to the UK Supreme Court.

The consequence of the potential disapplication of Section 13(2) of the DP Act by the Court of Appeal is that compensation is now recoverable by an individual under Section 13(1) for any damage that is suffered by the individual as a result of a breach of the DP Act by the Data Controller. Therefore individuals can now receive compensation from a Data Controller for distress without needing to demonstrate they have also suffered pecuniary loss.

Criminal offence for Enforced Subject Access brought into force

From 10 March 2015 it is a criminal offence under Section 56 of the DP Act to require an individual to exercise their subject access rights under the DP Act in order to access information about their convictions and cautions and for such information to be provided to a person, such as a prospective employer. This practice is commonly known as enforced subject access which typically occurs when a person wishes to see another individual's criminal record but does not use the established criminal records disclosure regime.

New ICO Code of Practice on Conducting Privacy Impact Assessments

The ICO has published a new code of practice on conducting privacy impact assessments ("PIA"). A PIA is a process which helps an organisation to identify and minimise the privacy risks associated with a project. It is not a legal requirement to conduct PIAs under the DP Act. However, the ICO states in the Code of Practice that conducting a PIA will assist in ensuring that new projects comply with the requirements of the DP Act and the ICO promotes
the use of PIAs as a tool to help organisations with such requirements. In
addition, the ICO states in the Code of Practice that it may often ask an
organisation whether it has carried out a PIA and PIAs are often an effective
way of demonstrating to the ICO how personal data processing complies with
the requirements of the DP Act. The Code of Practice provides guidance on
the steps in the PIA process, which include identifying the need for a PIA,
describing the information flows, identifying privacy and related risks,
determining and evaluating the privacy solutions, sign off and recording PIA
outcomes, integrating outcomes into the relevant project plan and consulting
with internal and external stakeholders throughout the process. The Code of
Practice also includes a template that can be used to help produce a privacy
impact assessment report.

2. Emerging Privacy Issues and Trends

ICO Enforcement Action

In the period between January 2014 and April 2015, the ICO has issued
13 monetary penalties for serious breaches of the E-Privacy Regulations or
the DP Act. The ICO issued 6 monetary penalties for breaches of the
electronic direct marketing rules contained in the E-Privacy Regulations, 5 of
which related to nuisance telephone calls, and the fines ranged from £50,000
to £90,000. In addition, 1 fine was issued during this period for breaches
related to unwanted text messages which amounted to £70,000. The ICO is
particularly focused on enforcing the electronic direct marketing rules under
the E-Privacy Regulations especially in relation to telephone calls and text
messages, which is driven by the number of complaints that the ICO receives.
As mentioned above, given the recent change to the E-Privacy Regulations it
is likely that the ICO will continue its focus on enforcement action in this area.

As in previous years, the ICO has continued to issue monetary penalties for
serious breaches of the DP Act, the majority of which relate to data security
breaches. The ICO issued 7 fines for such breaches of the DP Act from
January 2014 to April 2015, 4 of these related to organisations which were
subject to an online attack where third parties gained unauthorised access to
personal data, often including either highly sensitive personal data or credit
card information. The fines that were issued ranged from £7,500 (this would
have been £75,000 but was reduced by the ICO due to mitigating
circumstances) to £200,000. The ICO issued 3 fines for other types of security
breaches, which involved the sale of a filing cabinet at an auction which
included files containing sensitive personal data, the sale of a police station
which included tapes and other documents containing sensitive personal data
and the loss of an unencrypted hard drive containing sensitive personal data.
The fines for these breaches were £185,000, £100,000 and £180,000
respectively.
3. Law Applicable


4. Key Privacy Concepts

a. Personal Data

The DP Act applies to the processing of any data ("Personal Data") relating to an identified or identifiable living individual ("Data Subject"). The ICO has issued guidance on the classification of data as Personal Data. In general, the guidance suggests that in most cases it will be obvious whether or not data will be considered Personal Data. The primary question to consider is “Can a living individual be identified from the data, or, from the data and other information in the possession of, or likely to come into the possession of, the Data Controller?”

The ICO has also issued guidance with a view to clarifying what is “data” for the purposes of the DP Act. The guidance aims to help organizations determine whether information falls within any of the four categories of data covered by the DP Act: automatically processed data; data forming part of a relevant filing system; data forming part of an accessible record; and data recorded by a public authority.

b. Data Processing

“Processing” is extremely widely defined and covers any operation or set of operations performed on Personal Data including collection, recording, organization and deletion. The DP Act applies to both manual and automated data processing.

c. Processing by Data Controllers

The DP Act applies to those persons who determine the purposes for which and the manner in which any Personal Data is, or is to be, processed ("Data Controller").

d. Jurisdiction/Territoriality

The DP Act applies to data processing activities carried out by:

- Data Controllers established in the UK; and
• Data Controllers that are not established in the EEA but that use equipment located in the UK to carry out data processing activities (other than merely for the purpose of transit).

The ICO has indicated that “use of equipment” may include, for example, the hosting of a website within the UK or the use of cookies (i.e. if cookies are placed on the computers of internet users within the UK).

e. Sensitive Personal Data

The DP Act imposes additional requirements for the processing of sensitive Personal Data – that is, Personal Data relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health or condition, sexual life, commission or alleged commission of any offense, or criminal proceedings. Specifically, the processing of sensitive Personal Data is prohibited unless one of a number of stated conditions is met. These include:

• the Data Controller obtains the explicit consent of the Data Subject (see Section 5(b) below);

• the processing is necessary to carry out the obligations or rights of the Data Controller in connection with employment;

• the processing is necessary to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent or the Data Controller cannot reasonably be expected to obtain consent;

• the processing is carried out in the course of legitimate activities by any body or association which is not established or conducted for profit and which exists for political, philosophical, religious or trade union purposes and provided other specific conditions of processing are met;

• the information contained in the Personal Data has been made public as a result of steps deliberately taken by the Data Subject;

• the processing is necessary for the purpose of legal proceedings, obtaining legal advice or for establishing, exercising or defending legal rights;

• the processing is necessary for the administration of justice, for the functions of Parliament, for the exercise of powers conferred on a person under an enactment or for the exercise of functions of the Crown, a Minister or of a government department;

• the processing is necessary for medical purposes and is undertaken by a health professional or person with the equivalent duty of confidentiality as a health professional;
• the processing is of sensitive Personal Data consisting of information on racial or ethnic origin and is necessary for reviewing and ensuring equality of opportunity and treatment between different racial or ethnic origins and provided appropriate safeguards for the rights and freedoms of Data Subjects are in place; or

• the information is about a criminal conviction or caution, and the processing is necessary for the purpose of administering an account relating to a payment card (or for cancelling the payment card) used in the commission of one of certain listed offenses relating to indecent images of children and for which the Data Subject has been convicted or cautioned under the relevant legislation in England and Wales, Scotland or Northern Ireland.

f. Employee Personal Data

Employers inevitably have to process both sensitive and non-sensitive Personal Data about their employees. Sensitive data in the employment context typically consists of information relating to employees’ physical or mental health, sexual life, religion, racial or ethnic origin, and trade union membership, etc.

The ICO has published a detailed Employment Practices Code which is a practical guide to how the ICO considers employers can comply with the DP Act in relation to employee data. The Code is not legally enforceable, but will be taken into account by courts when enforcing the DP Act and, therefore, compliance with it is very much recommended.

Provided that the employer is careful about the type of data that it obtains from employees and complies with the data protection principles set out in the DP Act (e.g. the data collected is adequate, relevant and not excessive and is processed for limited purposes), the employer is generally able to justify processing non-sensitive employee Personal Data without the need to obtain employee consent (consent of the Data Subject is one of the conditions for processing non-sensitive Personal Data set out in the DP Act). It can do so if one of the other processing conditions set out in the DP Act are met, for example, if: (i) it is necessary to perform the employment contract; (ii) it is necessary to comply with a legal obligation to which the employer is subject; or (iii) it is in the employer’s legitimate interests and does not unduly prejudice the employee’s right to privacy or other rights.

The restrictions on processing sensitive employee Personal Data are more stringent. In order to do so, additional processing conditions must be met. For example, the employer can process sensitive Persona Data where it is necessary: (i) to perform or exercise any right or obligation imposed by law in connection with their employment; (ii) for the purpose of or in connection with legal proceedings or to obtain legal advice; or (iii) to establish, exercise or defend legal rights. For example, health information can be processed for the
purposes of ensuring the employee is kept safe at work and appropriate adjustments are made to their working environment, and information about an employee’s ethnic or racial origin may be processed for the purpose of meaningful equal opportunities monitoring, although typically that should be done in an anonymized form whenever practicable.

Where the other processing conditions cannot be met, a fallback justification for processing both sensitive and non-sensitive employee Personal Data is obtaining employee consent (or “explicit” consent in the case of sensitive Personal Data). However, this is not recommended, partly because of the difficulties of obtaining every employee’s consent, and also because the ICO has expressed significant doubts about the validity of consent in the employment context, because of the inequality of bargaining power.

In addition to the above, employers should ensure that all employee personal and sensitive Personal Data is accurate and up to date, is kept securely, and is not retained for longer than is necessary (see Sections 8 and 12 below).

5. Consent

a. General
Consent of the Data Subject is not mandatory although it is contemplated as a justification for processing, and in practice can be one of the more straightforward ways to justify processing. Written consent is not required. Consent is not defined in the DP Act. However, the ICO’s Legal Guidance on the DP Act explains that:

- in order for the Data Subject to signify his/her agreement to Personal Data relating to him/her being processed, there must be some active communication between the parties;
- the adequacy of any consent or purported consent must be evaluated; and
- consent must be appropriate to the particular circumstances.

b. Sensitive Data
Where consent is relied upon to justify the processing of sensitive Personal Data, it must be explicit and must be obtained prior to processing. The ICO’s Legal Guidance on the DP Act explains that “explicit consent” must be absolutely clear and should cover the specific detail of the processing, the particular type of Personal Data to be processed (or even the specific information in question), the purposes of the processing and any special aspects of the processing which may affect the individual. (See Section 4(e))
c. Minors
The DP Act does not specify a minimum age at which a child can provide valid consent. The ICO has, moreover, taken the view that to attempt to do so would not be advisable, as much will depend on the capacity of the child and the complexity of the proposition that is being put to him. On this point (and specifically in the context of the online processing of Personal Data), the ICO has stated that “assessing understanding, rather than merely determining age, is the key to ensuring that Personal Data about children is collected and used fairly.” There is a distinction drawn, however, between children under the age of 12, who are considered incapable of providing valid consent to the processing of their Personal Data (and in respect of whom the explicit and verifiable consent of a parent or guardian will always be required), and children between the ages of 12 and 16. In the case of the latter, the ICO considers that such a child may be capable of providing valid consent if the information collected is restricted to that necessary to enable the child to be sent further but limited communications and it is clear that the child understands what is involved. That said, the position for children between 12 and 16 is recognized as a “grey area” and the above is offered as guidance only and should not be assumed to apply in all cases. For example, the ICO has stated (again in the context of the online processing of Personal Data) that organizations may decide to obtain parental consent for children aged over 12 where there is a greater risk. In the case of children over 16, there is a presumption that they are capable of providing valid consent.

d. Employee Consent
In the UK, there are doubts as to whether consent given in the context of an employment relationship can be considered valid. It is questionable whether consent would qualify as voluntary, given that the employee may feel forced to consent due to the subordinate nature of their relationship with their employer.

An employer can process Personal Data without employee consent if one of the other processing conditions set out in the DP Act are met, for example, if: (i) it is necessary to perform the employment contract; (ii) it is necessary to comply with a legal obligation to which the employer is subject; or (iii) it is in the employer’s legitimate interests and does not unduly prejudice the employee’s right to privacy or other rights. However, there are stricter requirements when employers are processing employee’s sensitive Personal Data (see Section 4(f)).

e. Online/Electronic Consent
In the UK, online or electronic consent is permissible and deemed effective if properly structured and evidenced.
6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information on: the name of the Data Controller; the purposes for which the data is intended to be processed; and any additional information which is necessary to ensure that the processing is fair in the circumstances (this might include the identity of any third parties to whom the Personal Data may be transferred). Where data is obtained from a third party, the Data Controller will not have to provide this information where to do so would involve “disproportionate effort” or where collection or disclosure of the data is necessary for the Data Controller’s compliance with a legal obligation.

7. Processing Rules

A Data Controller is required to process Personal Data fairly and lawfully. Personal Data can only be obtained for one or more identified purpose(s) and must not be further processed in any manner which is incompatible with those purposes. Data Controllers must ensure that Personal Data is adequate, relevant and not excessive in relation to the purposes for which it is processed. Data Controllers must not keep Personal Data for longer than is necessary for the purpose for which it is processed. Data Controllers must ensure that Personal Data is accurate and where necessary kept up to date. In addition, Data Controllers must adopt appropriate technical and organizational security measures (see Section 12), comply with the rules regarding international data transfers (see Section 11) and respect the rights of Data Subjects (see Section 8).

8. Rights of Individuals

Data Subjects have the right to: be informed by a Data Controller upon written request of the Personal Data which the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data in certain limited circumstances.

9. Registration/Notification Requirements

Data Controllers are required to file a notification with the ICO, which maintains a public register of Data Controllers.

10. Data Protection Officers

In the UK, there is no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.
11. International Data Transfers

Transfers of Personal Data from the UK to EEA Member States are generally permitted without the need for further approval. Transfers are also permitted to Canada, Argentina, Guernsey, the Isle of Man, Jersey, the Faroe Islands, Andorra, Israel, Switzerland, New Zealand and Uruguay, which are the subject of the European Commission's findings of adequacy (subject to the fulfillment of certain pre-conditions) in relation to their data protection laws. Transfer to the US is permitted where the recipient has signed up to the Safe Harbor arrangement.

Subject to the specific authorizations mentioned above, Personal Data may not be transferred to countries outside the EEA, unless the destination country provides adequate protection of the Personal Data. Exceptions to this general prohibition are, however, expressly contemplated under the DP Act, including where:

- the Data Subject has consented to the transfer;
- the transfer is necessary to perform a contract with the Data Subject, or to take steps at his request with a view to entering into a contract with him;
- the transfer is necessary for the conclusion or performance of a contract entered into between the Data Controller and third parties in the interests of, or at the request of, the Data Subject;
- the transfer is necessary to protect the vital interests of the individual, or for reasons of public interest, or in connection with legal proceedings, or for the purpose of obtaining legal advice or establishing, exercising or defending legal rights; or
- the transfer has been specifically authorized by the ICO, or is made on terms which are of a kind approved by the ICO. This is the language in the DP Act itself. In practice, however, the ICO has indicated it does not propose to approve any forms of terms for the transfer of Personal Data.

The adoption of model contractual clauses approved by the European Commission will also provide an adequate level of protection to justify the transfer. (Note that the Data Controller must in any event justify all of its data processing under the DP Act; justification of any transfers is an additional compliance requirement.) Unlike many other EU Member States, if a transfer contract is used it will not need to be filed or approved by the ICO, whether before or after any transfers take place.

Where multinational organizations are transferring personal information outside the EEA, but within their group of companies, they may also adopt BCR as a means of justifying such intra-group transfers. Acceptable BCR may include intra-group agreements, policies or procedures, and special
arrangements among the group of companies that afford the requisite protection. The ICO, along with twenty other DPAs across the EEA have agreed to mutually recognize BCRs approved by one of these 21 DPAs. For BCR to enable the transfer of personal information freely within a corporate group, they must be approved by at least one DPA that has agreed to mutually recognize BCR applications, and by any remaining DPAs in EEA countries from which the organization transfers Personal Data and which have not agreed to mutual recognition of BCR applications. The Article 29 Working Party has adopted a model checklist and table setting out the required contents of an application to a data protection authority for approval of proposed BCR. As at May 2015, a total of 22 BCR authorizations had been granted by the ICO.

12. Security Requirements

Data Controllers are required to take steps to ensure that Personal Data in its possession and control (and where processed by a Data Processor on the Data Controller’s behalf) are protected from unauthorized or unlawful access and use and accidental loss, destruction or damage; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved and the harm that may result from unauthorized or unlawful access and use and accidental loss, destruction or damage.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Where Personal Data is processed on behalf of a Data Controller, the Data Controller is under an obligation to: (a) ensure that it has chosen a Data Processor which provides sufficient guarantees in respect of the technical and organizational security measures governing the relevant processing; (b) take reasonable steps to ensure compliance by the Data Processor with those measures; and (c) enter into a written contract with the Data Processor which requires the Data Processor to act only on instructions from the Data Controller, and to comply with obligations equivalent to those imposed on the Data Controller with regard to adopting appropriate technical and organizational measures against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data (including taking reasonable steps to ensure the reliability of any employees who have access to the Personal Data). In addition, if the Data Processor is located outside the EEA the contract with the Data Processor will need to address the issues outlined in Section 11 above.

Also, guidance from the ICO emphasizes the importance of the Data Controller’s due diligence and on going monitoring (e.g. regular reports or inspections) of the Data Controller’s preferred Data Processor.
14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

The E-Privacy Regulations require providers of public communications services (e.g., telecoms operators and internet service providers) to notify the ICO of security breaches which lead to the loss or disclosure of personal data and also to notify the relevant individuals if the breach is likely to affect their privacy. This notification obligation applies to all security breaches, and not just serious breaches. As a result of the Commission Regulation (EU) 611/2013 (“Notification Regulation”), such security breaches must be notified to the ICO within 24 hours of detecting a breach, along with information about the breach (where feasible). In addition, full details of the security breach need to be provided to the ICO within 3 days but where this is not possible a justification for the delay must be provided to the ICO with full details to follow without undue delay. In addition, although not required by the E-Privacy Regulations, the ICO has stated that organizations should also submit the log of breaches (required to be maintained under the E-Privacy Regulations) to the ICO on a monthly basis. The ICO has published guidance in relation to the notification of security breaches required under the Privacy Regulations as a result of Commission’s Notification Regulation.

Other than the obligations on telecoms operators and internet service providers, there is currently no other general obligation on Data Controllers to notify either individual Data Subjects or the ICO in the event of a data security breach. However, the ICO has issued guidance which sets out the circumstances in which serious data security breaches should be notified to the ICO. In addition, specific sectors may be subject to specific legal or regulatory requirements or codes of practice which in some circumstances require notification of security breaches.

16. Accountability

There is no current law in the UK that requires organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. However, the ICO has published a code of practice on conducting privacy impact assessments which sets out the basic steps an organization should carry out during the assessment process and includes a template that can be used to help produce a privacy impact assessment report.

17. Whistle-blower hotline

Whistle-blower hotlines may be established in the UK provided that they comply with local laws.
18. E-discovery

When implementing an e-discovery system, an organization is required to advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to ensure that any interception is proportionate (i.e., does not entail blanket monitoring), is for a legitimate business purpose and that notice is provided to all users.

20. Cookies

There are specific laws/rules that regulate the deployment of cookies, and hence, the use of cookies must comply with data privacy laws. Consent must be obtained before cookies can be used, other than for cookies which are strictly necessary for the service requested by the user. The ICO has stated in its guidance that implied consent can be relied upon in certain circumstances.

21. Direct Marketing

Both the DP Act and E-Privacy Regulations contain rules on direct marketing and the ICO has also published guidance on these rules. The ICO indicates that where consent is required for direct marketing, organizations must be able to demonstrate that consent was knowingly given, clear and specific, and organizations should keep clear records of such consent. The ICO recommends that organizations should use opt-in boxes if possible. The ICO also highlights that the rules on calls, texts and emails are stricter than the rules on mail marketing, and consent in relation to marketing via calls, texts and emails must be more specific. The ICO discourages organizations from taking a one-size-fits all approach in relation to direct marketing. The ICO emphasises the importance of carrying out rigorous checks before relying on indirect consent (e.g., consent originally given to a third party) and that indirect consent is unlikely to be sufficient for direct marketing via calls, texts or emails, particularly if the consent is generic or non-specific. In addition, the ICO states that organizations must not carry out automated pre-recorded marketing calls without specific prior consent and must not send marketing texts or emails to individuals without their specific prior consent (with the limited exception for existing customers for similar services).
United States

Amy de La Lama  
Chicago  
Tel: +1 312 861 2923  
amy.delalama@bakermckenzie.com

Lothar Determann  
Palo Alto  
Tel: +1 650 856 5533  
lothar.determann@bakermckenzie.com

Michael Egan  
Washington, D.C.  
Tel: +1 202 452 7022  
michael.egan@bakermckenzie.com

Marc Elzweig  
San Francisco  
Tel: +1 415 576 3018  
marc.elzweig@bakermckenzie.com

Brian Hengesbaugh  
Chicago  
Tel: +1 312 861 3077  
brian.hengesbaugh@bakermckenzie.com

Heather Mantegna  
Chicago  
Tel: +1 312 861 8808  
heather.mantegna@bakermckenzie.com

Lindsay Martin  
Chicago  
Tel: +1 312 861 2949  
lindsay.martin@bakermckenzie.com

Brandon Moseberry  
Chicago  
Tel: +1 312 861 8265  
brandon.moseberry@bakermckenzie.com

Karen Sewell  
Chicago  
Tel: +1 312 861 8228  
karen.sewell@bakermckenzie.com

Michael Stoker  
Chicago  
Tel: +1 312 861 2870  
michael.stoker@bakermckenzie.com
Although the United States does not have a comprehensive federal data protection law, every business in the United States is subject to privacy laws at the federal and/or state level. California in particular has been very active in passing new privacy laws in the last few years and we have added a separate chapter on California privacy laws to the 2015 Edition of this Handbook. Many federal and state privacy laws apply also to companies that are based in other countries and collect personal data from people in the United States, for example, via the Internet or mobile apps. U.S. federal and state privacy laws and other privacy requirements are actively enforced by federal and state authorities, and are aggressively enforced via class action lawsuits and privacy-related litigation.

1. A Multitude of Federal and State Privacy Laws

The first challenge that any business faces in the United States is to identify the privacy laws that apply to its business operations. There are a multitude of federal and state privacy laws. Some privacy laws focus on particular industries, such as: (i) healthcare privacy rules under the Health Insurance Portability and Accountability Act and comparable state laws; (ii) financial services privacy rules under the Gramm-Leach-Bliley Act and comparable state laws; and (iii) telecommunications privacy rules for customer proprietary network information under the Telecommunications Act of 1996.

Some privacy laws focus on particular activities, such as: (i) the Fair Credit Reporting Act that applies to companies that gather and share certain data about consumers for credit, employment and other specified purposes (“consumer reporting agencies”), as well as companies that use the consumer reports (“users”), companies that furnish data to consumer reporting agencies (“furnishers”), employers who use consumer reports for background check purposes and other businesses that engage in certain activities (such as printing consumer credit card numbers on receipts); (ii) the Children’s Online Privacy Protection Act that applies to companies that engage in online collections of personal information about children under 13; and (iii) the Electronic Communications Privacy Act and comparable state laws that generally apply to, among other activities, the interception of wire, oral, or electronic communications, and access to certain stored communications.

Some privacy laws focus on particular data types, such as certain laws in California and Massachusetts, and a large number of other state data security and breach notification requirements that apply to Social Security Numbers, bank account numbers, credit card numbers, health information, and a broad range of other sensitive data fields.

2. Federal Trade Commission and State Attorneys General

Beyond the specific privacy laws and regulations, the Federal Trade Commission (“FTC”) has broad authority pursuant to Section 5 of the FTC Act to take action against businesses that engage in certain “unfair or deceptive”
trade practices. The FTC has traditionally used this authority to pursue companies that engage in “deceptive” practices, such as violating consumer privacy policies. In recent years, the FTC has expanded the use of its authority to take actions against companies that engage in “unfair” practices, meaning practices that are disclosed in a privacy policy, but nevertheless are deemed by the FTC to be contrary to consumer expectations or otherwise harmful. The trend toward more robust enforcement that moves beyond merely enforcing the company’s privacy policy is continuing. In a recent case, *FTC v. Wyndham Hotels*, the FTC prevailed against complaints that it is exceeding its authority by creating federal privacy law without a legislative mandate to do so. The outcome of the case has encouraged the FTC’s ability to continue and expand its efforts and even more aggressively exercise its fairness enforcement power in privacy and security cases.

For these reasons, businesses must address FTC actions in the form of a growing body of FTC privacy consent decrees, as well as FTC guidance on privacy matters. The FTC has started the new year in 2015 by issuing a report on the “Internet of Things” and urging companies to adopt best practices to address consumer privacy and security risks. Also relatively new and worth noting is the FTC’s 2014 guidance on privacy protection for children online, which affirmatively states that the U.S. Federal Children Online Privacy Protection Act applies to foreign companies that collect personal data from children in the United States, U.S. companies that collect personal data from children abroad and companies that act as mere data processors or collect data about children under 13 via cookies on third party websites.

Also still relevant is the FTC’s 2012 report on “Protecting Consumer Privacy in an Era of Rapid Change” (the “Report”).

The Report outlines a proposed framework that applies to nearly all commercial entities that collect (either online or offline) or use consumer data that can reasonably be linked to a specific consumer, as well as to data about a specific computer or other device. The scope is not limited to collections of “personally identifiable data,” because, according to the FTC, there is no longer a clear distinction between personally and non-personally identifiable data since anonymized or de-identified data can now frequently be linked to the relevant individual. For example, data stored in a cookie that shows the websites a user previously visited would fall within the scope of the framework, as would data linked to the Unique Device Identifier or “UDID” for a mobile device. The Report states that certain de-identified data will not be considered “reasonably linked” to the individual, in particular if the company takes certain measures to de-identify the data and ensures that it cannot be re-identified.

The framework identifies the following three core privacy principles for companies to follow in their privacy practices: (1) *privacy by design*; (2) *simplified choice*; and (3) *greater transparency*. 
With respect to privacy by design, companies must build privacy protections into their everyday business practices. Specifically, companies must:
(i) incorporate substantive privacy protections into their practices (e.g., data security, reasonable collection limits, sound retention practices and data accuracy); and (ii) maintain comprehensive data management procedures throughout the life cycle of their products and services. Depending on the size of the company and the volume and sensitivity of personal data, such practices might include assigning personnel to oversee privacy issues, training employees on privacy issues and conducting privacy reviews when developing new products and services.

Regarding simplified choice, companies must provide choices to consumers about their data practices in a simple and streamlined manner. To achieve this goal, consumer choice must be provided in certain situations and not in others. In particular: (i) consumer choice must not be provided before companies collect and use consumer data for “commonly accepted practices”, such as product and service fulfillment, internal operations such as product improvement, fraud prevention, legal compliance, and first-party marketing; (ii) for all other practices, consumer choice must be provided and such choice should be offered at a time and in a context in which the consumer is making a decision about his or her data (e.g., at the time when the data is actually collected rather than in the privacy policy); (iii) for “sensitive data”, including health and medical data, express opt-in consent must be obtained for the collection and use of such data; and (iv) for online behavioral advertising, the FTC encourages the development of a “do-not-track” framework as a key option for adequately addressing consumer choice issues in this context.

With respect to the promotion of greater transparency, companies must:
(i) issue privacy notices that are clearer, shorter and more standardized;
(ii) provide individuals with reasonable access to the data that they maintain, where the extent of the access should be determined based on the sensitivity of the data and other factors; (iii) provide prominent disclosures of changes in uses of data and obtain user consent before using data in a materially different way than was disclosed at the time of collection; and (iv) educate consumers about their data privacy practices.

Beyond the FTC actions, many State Attorneys General also have broad authority to pursue unfair or deceptive practices pursuant to state powers (often called “Mini-FTC Acts”). An important recent trend has involved greater collaboration between and among State Attorneys General to pursue actions against companies that experience data security breaches or other privacy issues. Such coordinated actions can often exact greater penalties and impose increased demands on companies than what would otherwise be required by the FTC.
3. US Law Enforcement and Other Legal Demands

Beyond federal and state privacy laws, there are various related federal and state requirements to produce information to law enforcement and regulatory authorities, to gather data for purposes of global internal investigations, and to respond to e-discovery and other demands for data in civil litigation. By way of a few examples, companies may be ordered to produce information pursuant to: (i) a search warrant executed by federal or state criminal authorities; (ii) an order for the interception of electronic communications by criminal authorities pursuant to federal or state wiretap acts; (iii) a grand jury subpoena issued by federal or state criminal authorities; (iv) a trial subpoena issued by federal or state criminal authorities; (v) an administrative subpoena issued by federal or state regulatory authorities; (vi) a civil subpoena seeking the production of documents in connection with civil litigation; and (vii) another form of court order requiring disclosure, such as an order under Section 215 of the USA Patriot Act.

Some of these US legal demands, including orders under the USA Patriot Act, have attracted considerable attention in non-US jurisdictions and such attention has increased dramatically in the wake of the publicity about surveillance programs by the U.S. NSA and cooperating intelligence agencies in Australia, Canada, New Zealand and the UK (part of the “Five Eye” alliance) and other U.S. allies, including Germany (Bundesnachrichtendienst). The U.S. government has created various new administrative safeguards, including appointing privacy officers at the agencies and creating a privacy oversight board that has published a scathing report, declaring some of the existing programs unconstitutional and illegal under U.S. law. A number of lawsuits against these and other programs are working themselves through the U.S. court system with wins for plaintiffs, which include the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF) and support their efforts in reigning in the activities of the U.S. intelligence agencies. These government measures and court cases will help reduce the risk of potential conflicts with non-US data protection, privacy, bank secrecy, confidentiality, anti-investigatory or “blocking” statutes, and other data restrictions. In practice, companies need to be mindful of these potential conflicts when structuring their global privacy compliance programs. Also, when any such demand is received, the company should carefully assess options and approaches to help address the US and non-US requirements. For example, can the law enforcement authority at issue utilize any Mutual Legal Assistance Treaties (“MLATs”) to obtain the data directly from its counterparts in a foreign jurisdiction? Can the company assert that the data at issue is not within the company’s lawful control and therefore cannot be produced? Can the company persuasively argue against production of the data on the grounds that it may violate non-US privacy or other laws? These are a few examples, and each situation requires a careful assessment of the specific facts and the applicable US and non-US legal requirements.
4. Summaries of Key Privacy Laws

An exhaustive review of US privacy laws is outside the scope of this handbook. Instead, the following sections summarize key aspects of some key federal and state laws relating to data privacy. The federal laws covered are the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Children’s Online Privacy Protection Act. In addition, the handbook covers the data security regulations published by the Massachusetts Office of Consumer Affairs and Business Regulation and the security breach laws that have been enacted in most states, as illustrated by key provisions of California’s statute. As noted above, these examples do not represent an exhaustive list of applicable restrictions but are intended as illustrations of the laws and regulations that are currently in place in the United States.
United States
California Privacy Laws

1. Recent Privacy Developments

In the last two years, California has enacted more than 20 new privacy laws and updates to existing privacy laws, including:

- requirements on operators of websites (within or outside the United States) that collect personal data from California consumers to disclose how they respond to ‘Do Not Track’ signals and details on third party data collection;
- a limited ‘right to be forgotten’ for minors, requiring platform operators to enable minors to remove their own posts (but not posts reproduced by third parties);
- an extension of existing health information privacy laws to companies that offer software, hardware or online services to consumers for purposes of maintaining medical information;
- an expansion of the California data security breach notification law (covered in a separate chapter of this handbook); and
- laws intended to reign in revenge porn.

At the same time, plaintiffs law firms have increased privacy-related class action lawsuits in California courts based on California privacy laws, including laws:

- requiring consent from all parties before calls, emails or other communications including persons in California can be monitored, filtered or recorded;
- prohibiting retailers from collecting any personal data from credit card holders, even with consent, except as necessary to process credit card transactions (California Song Beverly Credit Card Act);
- requiring companies to disclose sharing of personal information with third parties (including affiliated companies operating under different brands) for their direct marketing purposes; and
- general unfair competition laws in the context of alleged misrepresentations in privacy policies, particularly representations regarding ‘reasonable data security measures’ in the aftermath of data security breaches.
2. Emerging Privacy Issues and Trends

Within the United States, California is usually the first to enact new legislation in the areas of data privacy and security and consumer protection more generally. California is world-renowned for innovation in the data processing and information technology fields as well as in the data privacy legislation arena. The state has successfully implemented various pieces of legislation requiring disclosures and transparency, such as California’s data security breach notification law and California’s Online Privacy Protection Act that requires companies to post privacy policies for online consumer services. Both laws were firsts worldwide and successfully copied around the world. Nearly all U.S. states and many foreign countries have data breach notification laws now.

Less successful and burdening businesses with a flurry of painful lawsuits have been some of California’s absolute prohibitions, like the California Song-Beverly Credit Card Act, and detailed prescriptions like the “Shine the Light” law that requires companies to post a text link with “Your Privacy Rights” on their home pages (a requirement that would unnecessarily clutter webpages if every jurisdiction were to require such special mention in the title of a text link).

3. Law Applicable

California has enacted more than a hundreds of sector-, activity- and data type-specific privacy laws, including some laws that have since been regulated on a federal U.S. level and potentially been pre-empted (such as California’s anti-spam laws and laws on health and financial privacy laws). Particularly relevant in practice remain the following California laws:

- Under the California Online Privacy Protection Act, operators of websites and online services within and outside the United States have to post privacy policies with certain prescribed disclosures if they collect personally identifiable information from consumers in California.

- Under the California Shine the Light Law, companies have to disclose certain details of their data sharing practices if they make personal information on California consumers available for direct marketing purposes of unaffiliated companies or affiliates operating under a different brand; companies can satisfy some requirements by posting a notices under a link entitled “Your California privacy rights” on their homepage.

- Under the Song Beverly Credit Card Act, retailers are prohibited from collecting personal information from credit card holders, even with consent, except as necessary to process credit card transactions or deliver goods or perform services.
• Under the *California Penal Code*, companies are prohibited from recording or monitoring calls or other communications involving persons in California, unless all persons consent.

• Under the California Civil Code, companies have to apply various data security measures and notify data security breaches, as discussed in more detail in our separate chapters on ‘United States - State Data Security Laws’ and ‘United States - State Data Security Breach Notification Laws’.

4. Key Privacy Concepts

a. Personal Data
California privacy laws do not use the term “personal data” but refer to various other terms, including “personally identifiable information,” “personal identification information,” and “personal information.” Each statute - and often each section in a statute - tends to define the relevant term differently and often with enumerated categories of personal data listed.

b. Data Processing
California privacy laws do not use the term “data processing” or any other similarly broad definition of “data processing,” unlike European data protection laws do. California defines in each statute - and often: each section of a statute - differently which data processing activities are covered by the particular law.

c. Processing by Data Controllers
Some California laws differentiate between data controllers and processors like European data protection laws do, e.g., regarding data security breach notification laws (processors must notify controllers and controllers must notify data subjects and the California State Attorney General), but, many laws do not differentiate or draw different lines.

d. Jurisdiction/Territoriality
California privacy laws apply to companies in other U.S. states and other countries in situations with a nexus to California (e.g., collection of personal data of consumers in California), unless a particular statute expressly states that its applicability is limited to companies in California (e.g., Section 637.7 of the California Penal Code prohibits “entities in this state” from attaching RFID tracking devices) or the applicability of the law is limited by Federal U.S. law (e.g., the ‘Dormant commerce Clause’ of the United States Constitution).

e. Sensitive Personal Data
California privacy laws afford special protections to U.S. Social Security Numbers (because of identity theft risks), credit card and banking information, health information and certain other statutorily defined data categories.
f. **Employee Personal Data**

Under the California Labor Code, employers are prohibited from recording video or audio of employees in restrooms or changing rooms, regardless of employee consent. Otherwise, employee privacy is only protected where employees have reasonable privacy expectations, which employers can - and usually do - negate with detailed privacy notices.

5. **Consent**

a. **General**

Companies are generally permitted to collect and process personal data without consent. Many California privacy laws require conspicuous notice and courts tend to assume implied consent if data subjects continue showing up for work, using a service or continuing other conduct after they receive notice.

b. **Sensitive Data**

California privacy laws afford special protections to U.S. Social Security Numbers (because of identity theft risks), credit card and banking information, health information and certain other statutorily defined data categories, but do not typically require consent. Notices tend to suffice.

c. **Minors**

California law requires operators of websites and other online services to enable minors to remove social media posts. Certain types of advertisements may not be targeted at minors.

d. **Employee Consent**

Employee privacy is only protected where employees have reasonable privacy expectations, which employers can - and usually do - negate with detailed privacy notices. Affirmative or express consent is not generally required, except in certain limited scenarios, e.g., tracking of employee location with RFID technology.

e. **Online/Electronic Consent**

If and to the extent notice or consent is required, it can generally be provided electronically.

6. **Information/Notice Requirements**

In general, companies should provide detailed, accurate and conspicuous privacy notices under California law to protect and defend against charges of unfair or misleading business practices. Under most of the numerous California privacy laws, companies can defend themselves if they can prove that data subjects did not have a reasonable expectation of privacy. Privacy expectations can be defined, qualified or negated in notices. Therefore, privacy notices are the single most crucial measure under California privacy laws.
The risk of lawsuits arising from outdated, inaccurate or incomplete privacy notices under California law is much higher than in other jurisdictions, notably Europe.

A number of California privacy laws prescribe notice content and placement in a lot of detail. For example, under the California Online Privacy Protection Act, operators of websites and online services within and outside the United States have to post privacy policies with certain prescribed disclosures if they collect certain types of personally identifiable information from consumers in California (including potentially location information of data subjects collected on a no name basis). In the privacy policies, companies must notify consumers about (1) data categories collected, (2) processes to review and request changes (3) change notification, (4) the policy’s effective date, (5) responses to “do not track” signals or similar mechanisms, and (6) third parties’ data collection about consumer online activities over time and across different websites.

7. Processing Rules

In addition to various sector- and data type-specific rules on data processing, California privacy laws impose numerous data security requirements that we discuss in more detail in our separate chapters on ‘United States - State Data Security Laws’ and ‘United States - State Data Security Breach Notification Laws.’

8. Rights of Individuals

Most California privacy laws provide for a right of private action that can be enforced by way of class action lawsuits. The California Song Beverly Credit Card Act and a few other laws provide for statutory penalties, so plaintiffs’ attorneys do not have to substantive individual damages.

9. Registration/Notification Requirements

None.

10. Data Protection Officers

Not generally required, but many California companies appoint privacy officers for practical reasons.

11. International Data Transfers

Not restricted.

12. Security Requirements

Discussed in more detail in our separate chapters on ‘United States - State Data Security Laws’ and ‘United States - State Data Security Breach Notification Laws.’
13. Special Rules for the Outsourcing of Data Processing to Third Parties

None.

14. Enforcement and Sanctions

Companies are particularly sensitive to exposure to private lawsuits, including class action lawsuits that are very common and tend to result in judgments, settlements and legal fees in the millions of U.S.$s. The California State Attorney General has created a “Privacy Task Force” in 2012, which has launched criminal and civil actions against companies and individuals relating to a number of violations, including failure to post privacy policies and issue timely data security breach notifications.

15. Data Security Breach

Discussed in more detail in our separate chapter on ‘United States - State Data Security Breach Notification Laws.’

16. Accountability

Not specifically legislated or regulated.

17. Whistle-Blower Hotline

All public companies and more and more private companies in California operate whistleblower hotlines. Companies that operate whistleblower hotlines are not required to obtain any government approvals or submit government filings and are less exposed to privacy-related concerns as, for example, in Europe.

18. E-Discovery

Defendants can be compelled to produce documents and information relatively easily under California rules of civil procedure, compared to other jurisdictions. Defendants can try to protect data privacy via protective orders in this context, but rarely oppose information production obligations based on privacy theories.

19. Anti-Spam Filtering

Monitoring and filtering of electronic communication requires all party consent. Plaintiffs have challenged email filtering for marketing purposes under California and U.S. Federal privacy laws with some success, but not with respect to anti-spam or anti-virus filtering, which is generally believed not to interfere with reasonable privacy expectations and therefore to be generally permitted.
20. Cookies
Cookies are not specifically regulated under California privacy laws, but a number of companies have been sued based on unfair competition and misrepresentation theories for failure to provide adequate disclosures regarding cookies in privacy policies, attempts to disable consumer attempts to block or delete certain types of cookies and placement of certain particularly intrusive tracking technologies without consent. Based on recent updates to the California Online Privacy Protection Act, operators of websites and online services must disclose in privacy policies how they respond to “Do Not Track” Signals and similar privacy protection measures selected by consumers and if and to what extent third parties collect personal information regarding consumers on websites or via online services.

21. Direct Marketing
The California “Shine the Light Law” requires companies to provide certain disclosures if they share personal information with other companies for their direct marketing purposes, even to affiliated companies operating under a different brand.

California’s opt-in consent requirements have been largely pre-empted by the federal CAN-SPAM Act, which requires that companies provide certain disclosures, allow and honor opt-out requests and refrain from certain forms of email address harvesting, but which does not require opt-in consent.
United States
Children’s Online Privacy Protection Act (“COPPA”)

1. Recent Privacy Developments
The Federal Trade Commission (“FTC”) actively enforced COPPA in 2014. Areas of particular attention included:

- General audience sites (i.e., sites not explicitly directed at children) that triggered COPPA’s parental notice and consent requirements by collecting date of birth from users without blocking users from their sites who entered dates of birth that would make them under the age of 13.

- Child-directed apps offering games that also collected personal information such as geo-location and e-mail address without obtaining parental consent.

2. Emerging Privacy Issues and Trends
See Section 1 above.

3. Law Applicable
The Children’s Online Privacy Protection Rule (16 C.F.R. § 312.1 et. seq.) (the “Rule”), effective 1 July 2013, implementing the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et. seq.) (the “Act”), along with the FTC’s Frequently Asked Questions, providing guidance on how the FTC applies the Rule.

4. Scope of the Law
a. Personal Data
The Rule applies to the online collection of Personal Information from a child under the age of 13 (“Child” or “Children”). “Personal Information” is defined expansively and includes:

- first and last name;

- a home or other physical address, including a street name and name of a city or town;

- an e-mail address or other online contact information, including an instant messaging user identifier or a screen name that reveals an individual’s e-mail address;
• a telephone number;
• a Social Security Number;
• a persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;
• a photograph, video, or audio file where such file contains a child’s image or voice;
• geolocation information sufficient to identify street name and name of a city or town; or
• information concerning the Child, or the parent or legal guardian of that Child (“Parent”), that the Operator (see definition below) collects online from the Child and combines with an identifier described above.

b. Personal Information Collection
The Rule applies to the “collection” of Personal Information from a Child. “Collection” is broadly defined and applies to the online gathering of any Personal Information from a Child, including:
• requesting, prompting or encouraging a Child to submit Personal Information online;
• enabling a Child to make Personal Information publicly available through a chat room, message board, or other means (e.g., social networking/blogging), except where the Operator deletes all individually identifiable information from postings by a Child before they are made public, and also deletes such information from the Operator’s records; or
• the passive tracking or use of any identifying code linked to an individual such as a cookie.

c. Collection by Operator
The Rule applies to any operator of a website or online service that is directed to Children or to any other Operator with actual knowledge that it is collecting or maintaining Personal Information relating to a Child. An “Operator” is any person (or entity) who operates a website or an online service and who collects or maintains Personal Information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where the website or online service is operated for commercial purposes. Personal Information is collected on behalf of an Operator when it is either (1) collected or maintained by an agent or service provider of the Operator or (2) the Operator benefits by allowing another person to collect Personal Information directly from users of such website or
online service. A website “directed to children” means a commercial website, or portion thereof, that is targeted to Children. A website which refers or links to a commercial website or online service directed to Children by using information location tools, however, does not necessarily meet this definition.

d. **Jurisdiction/Territoriality**
The Rule applies to the collection of Personal Information about a Child by an Operator who engages in commerce: (a) across more than one State in the US; or (b) in any State in the US and in one or more foreign nations; or (c) in any territory of the US or in the District of Columbia; or (d) in any such territory and another such territory, State or foreign nation; or (e) in the District of Columbia and any State, territory, or foreign nation.

e. **Sensitive Personal Data**
Not applicable.

f. **Employee Personal Data**
Not applicable.

5. Consent Requirements

a. **General**
None.

b. **Sensitive Personal Information**
Not applicable.

c. **Parental Consent**
Prior to the collection, use, and/or disclosure of Personal Information about a Child, an Operator must obtain Verifiable Parental Consent from a Parent of the Child. The Rule explains that obtaining “Verifiable Parental Consent” means that the Operator must make any reasonable effort (taking into consideration available technology) to ensure that before Personal Information is collected from a Child, a Parent: (i) receives notice of the Operator’s Personal Information collection, use, and disclosure practices; and (ii) authorizes any collection, use, and/or disclosure of the Personal Information. In addition, the Operator must provide a Parent with the option of consenting to the collection and use of the Child’s Personal Information to the Operator without having to consent to its disclosure to a third party.

The Operator also must take steps to ensure that the person providing consent is actually the Child’s Parent. Acceptable forms of consent include (1) a consent form signed and returned by the Parent by mail or facsimile; (2) the Parent’s use, in conjunction with the transaction, of a credit card, debit card or other online payment system that provides notification of each discrete transaction to the primary account holder; (3) a call to a toll-free number provided by the Operator and staffed by trained personnel; (4) having a Parent
connect to trained personnel via video-conference; (5) verifying a Parent’s identity by checking a form of government-issued identification against databases of such information, where the Parent’s identification is deleted by the operator from its records promptly after such verification is complete; or (5) the electronic forms of consent discussed below.

d. **Minor Consent**

A Child cannot consent to the collection of his or her Personal Information. This consent must instead be obtained from a Parent of the Child. The Rule does not address consent requirements for minors who are 13 or over.

e. **Employee Consent**

Not applicable.

f. **Online/Electronic Consent**

If the Operator is not releasing the Personal Information to a third party, consent may be obtained by using e-mail coupled with additional steps to provide assurances that the person providing the consent is the Parent. Acceptable additional steps to obtain these assurances include sending a delayed confirmatory e-mail to the Parent following receipt of consent, or obtaining a postal address or telephone number from the Parent and confirming the Parent's consent by letter or telephone call. An Operator that uses this method must provide notice that the Parent can revoke any consent given in response to the earlier email.

g. **Exceptions to Prior Consent/Requirements**

In certain situations, the Operator is not required to obtain Parental consent before collecting and/or disclosing Personal Information about a Child. These situations include:

- where the Operator collects the name or online contact information of a Parent or Child to be used exclusively for obtaining Parental consent or providing Parental notice (the Operator must delete this information after a reasonable time if there is no response);

- where the Operator collects online contact information from a Child for the sole purpose of responding directly to a specific request from the Child on a one-time basis, and the Operator immediately deletes that online contact information immediately after responding to the Child;

- where the Operator collects online contact information from a Child to be used to respond directly more than once to a specific request from the Child;

- where the Operator collects a Child’s name and online contact information to the extent reasonably necessary to protect the safety of a Child participating on the website.
In all of the situations described above, except for where the Operator deletes the information after responding on a one-time basis to the Child, the Operator must provide notice and seek Parental consent after the Personal Information has been collected. Moreover, the Rule generally requires that the Operator delete all contact information after the relevant transaction has been concluded. An Operator also can provide notice and seek consent after the fact to the extent reasonably necessary to protect the security or integrity of its website, to take precautions against liability, to respond to a judicial process, to provide information to law enforcement agencies, or for an investigation on a matter related to public safety.

6. Information/Notice Requirements

The Operator must provide two types of notice. The Operator must post a prominent link to a notice of its information practices on its website’s homepage as well as any area where Personal Information is collected from Children. The notice must provide the following information:

- the contact information (name, address, telephone number, and email address) for all Operators collecting information about Children on the website;
- the types of Personal Information collected from Children and the manner of collection (passive v. active);
- how such Personal Information is or may be used by the Operator;
- whether the Personal Information is disclosed to third parties (and the types of businesses engaged in by such third parties, the purposes for which the Personal Information is used, and whether such parties are subject to agreements to protect the information);
- that the Parent has the option to consent to the collection and use of Personal Information without consenting to its disclosure to third parties;
- that the Operator is prohibited from conditioning a Child’s participation in an activity on the Child’s disclosing more Personal Information than is reasonably necessary to participate in the relevant activity; and
- that the Parent can review and have deleted his/her Child’s Personal Information and also refuse to permit collection or use of the Child’s Personal Information (the notice must also specify the corresponding procedures for doing so).

In most instances, the Operator also must provide notice directly to a Parent of the Child from whom it seeks to collect Personal Information before it collects such information. This notice must contain the information listed above. In certain limited situations, the notice may be provided after the information is collected.
7. Processing Rules

In general, the Rule prohibits unfair or deceptive acts or practices in connection with the online collection, use, and/or disclosure of the Personal Information of a Child.

8. Safe Harbor

An Operator will be deemed to comply with the Rule if it complies with self-regulatory guidelines that are issued by representatives of the marketing or online industries, or by other persons, which have been approved by the FTC. Industry groups must file a request with the FTC for approval of self-regulatory guidelines that meet the standards set out in the Rule – such requests are subject to notice and comment requirements prior to approval. Once approved, the self-regulatory program must submit annual reports regarding the efficacy of the program and any disciplinary action taken against any subject Operator. Any subsequent changes to the program also require prior FTC approval. In 2014, the FTC approved the iKeepSafe and kidSAFE Safe Harbor Program.

9. Rights of Individuals

a. Parent Access Rights

The Parent of any Child who has provided Personal Information to an Operator has the right to request access to such information. Upon receiving such a request, the Operator is required to provide the Parent with the following information:

- a description of the specific types or categories of Personal Information collected from the Child by the Operator, such as name, address, telephone number, e-mail address, hobbies, and extracurricular activities;
- the opportunity at any time to refuse to permit the Operator’s further use or future online collection of Personal Information from that Child, and to direct the Operator to delete the Personal Information collected from the Child; and
- a means of reviewing any Personal Information collected from the Child.

b. Child’s Rights

An Operator is prohibited from conditioning a Child’s participation in a game, the offering of a prize, or another activity on the Child’s disclosing more Personal Information than is reasonably necessary to participate in such activity.

c. Additional Rights

No specific requirements apply.
10. Registration/Notification Requirements
No specific requirements apply.

11. Data Protection Officers
Not applicable.

12. International Data Transfers
Not applicable.

13. Security Requirements
An Operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of Personal Information collected from Children. The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

14. Special Rules for the Outsourcing of Data Processing to Third Parties
Persons or entities who delegate or outsource the responsibility for collecting and maintaining Personal Information from a Child are still subject to the Rule.

15. Enforcement and Sanctions
Violations of the Rule are considered to be unfair or deceptive acts prohibited by the Federal Trade Commission Act and, consequently, are subject to FTC enforcement actions and/or financial penalties ($11,000 per violation). COPPA also gives States and certain other federal agencies authority to enforce compliance.

16. Data Security Breach
a. Are there any legal requirements, including notification obligations, in the event of a data security breach?
The Rule does not expressly identify such an obligation.

b. Risk of non-compliance
The Act gives states and certain federal agencies, including the FTC, authority to enforce compliance with the Act. A court can impose civil penalties of up to $11,000 per violation on website operators who violate the Rule.

17. Is there a filing requirement when a whistle-blower hotline is introduced in your jurisdiction?
Not applicable.
18. Would the implementation of an e-discovery system within an organization raise privacy issues?

Not applicable.

19. Would the introduction of a spam-filtering solution in an organization raise privacy issues?

Not applicable.
United States
Gramm-Leach-Bliley Act and Fair Credit Reporting Act

1. Recent Privacy Developments

The Bureau of Consumer Financial Protection (“CFPB”), the primary federal regulatory authority with power to administer the GLBA and FCRA (each as defined below), continues its rulemaking and advisory activities. The CFPB has issued guidance stating that the GLBA notice and opt-out requirements do not preclude disclosure of nonpublic personal information in the case of suspected financial abuse of older adults. (Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults.1 The guidance provides that such disclosures would fall under one or more of the exceptions to the requirements established under the GLBA. According to the guidance, such disclosures may be made at the request of a federal, state or local agency or upon the financial institution’s initiative. Additionally, amendments to Regulation P could be forthcoming from the CFPB.

The requirements of the FCRA are being actively enforced. The Federal Trade Commission (“FTC”) has engaged in active and consistent enforcement efforts against FCRA violations, giving particular attention to data brokers. In January 2014, the FTC reached a $3.5 Million settlement against TeleCheck Services, Inc., a consumer reporting agency, and an associated debt collection company, TRS Recovery Services, Inc.. Additionally, individuals have filed a substantial number of FCRA-related claims.

2. Emerging Privacy Issues and Trends

See Section 1 above.

3. Law Applicable


4. Scope of the Law

a. Personal Data

GLBA requires that “financial institutions” must protect certain non-public personal information collected from or about individual consumers in connection with the provision of financial products and services – it does not apply to information collected in other contexts. Non-public personal information includes personally identifiable financial information that:

- is provided by a consumer to a financial institution;
- results from any transaction with the consumer or any service preformed for the consumer; and/or
- is otherwise obtained by the financial institution.

A company’s obligations under GLBA depend on whether the company has consumers or customers who obtain its products or services. A consumer is an individual who obtains or has obtained a financial product or service from a financial institution for personal, family, or household reasons. A customer is a consumer with a continuing relationship with a financial institution. Generally, if the relationship between the financial institution and the individual is significant and/or long-term, the individual is a customer of the institution. For example, a person who gets a mortgage from a lender or hires a broker to get a personal loan is considered a customer of the lender or the broker, while a person who uses a check-cashing service is a consumer of that service.

FCRA primarily governs the uses and disclosure of information in “consumer reports.” The definition of a “consumer report” under FCRA is broad, and it incorporates by reference the definition of a “consumer reporting agency.” Analyzing both of these terms together, a consumer reporting agency generally is any person that: (a) for fees or other compensation, (b) regularly engages in the practice of assembling or evaluating “non-experience” information about consumers, (c) for the purpose of disseminating such information to third parties for use in connection with the evaluation of the consumer for credit, debt collection, or other “permissible purposes,” and (d) performs such activities in interstate commerce. See Porter v. Talbot Perkins Children’s Services, 355 F. Supp. 174 (SD NY 1973).

b. Data Processing

If a financial institution is within the scope of GLBA, the law will apply to the collection, use, storage, and any other activity that the institution undertakes with respect to non-public personal information.
FCRA applies to any collection, use, disclosure, or other processing of consumer reports by consumer reporting agencies. In addition, FCRA imposes certain obligations on entities that are “users” of consumer reports (e.g., use and disclosure limitations), as well as entities that furnish information to consumer reporting agencies (e.g., related to data integrity and correction of incorrect information), and various other requirements.

c. **Processing by Data Controllers**

GLBA does not contain a term “data controller” and instead coverage is defined by the term “financial institution,” as described above.

FCRA does not contain a term “data controller” and instead coverage is defined by the term “consumer reporting agency,” “user,” and “furnisher” as described above, as well as by other definitions.

d. **Jurisdiction/Territoriality**

GLBA does not contain a specific geographic limitation, but the jurisdictional reach is defined at least in part in the relevant regulations, and also by the jurisdictional reach of the relevant regulatory authority.

FCRA does not contain a specific geographic limitation, but the jurisdictional reach is defined at least in part by the jurisdictional reach of the relevant regulatory authority.

e. **Sensitive Personal Data**

GLBA does not include a classification of “sensitive” information, although collection of health or medical information may be subject to greater protection under state law implementation of GLBA in the insurance sector, and also may be subject to federal regulation in certain circumstances under other laws, such as the Health Insurance Portability and Accountability Act.

FCRA contains restrictions on collection, use, and disclosure of medical information and also contains special restrictions related to identity theft, consumer reports furnished for employment purposes, and a special category of consumer reports involving personal interviews with third parties termed “investigative consumer reports”.

f. **Employee Personal Data**

Employee personal data is generally not within the scope of GLBA, except in certain instances where the employee is a consumer of financial products or services provided by the employer or its affiliate, such as in the context of a company credit union. Under FCRA, a consumer reporting agency may generally not provide a consumer report to an employer, or a prospective employer, without that employee’s or prospective employee’s written consent. Additionally, employers performing background checks on prospective or existing employees must use specific, required forms provided under the applicable regulations.
5. Consent Requirements

a. General

GLBA generally requires a financial institution to provide customers and/or consumers in certain circumstances with a privacy notice with specified content. In situations where the financial institution intends to share non-public personal information with a non-affiliated third party, GLBA generally requires that the institution must provide the consumer with notice of the opportunity to opt-out of such disclosures, and must respect the expressed wishes of the consumer in this regard. There are important exceptions to these opt-out requirements, such as where the disclosure is necessary to effect, administer, or enforce the transaction, or where the disclosure is required or permitted by law. Providing some added clarity, the CFPB has issued guidance stating that disclosure in the case of suspected financial abuse of older adults would fall under one of the specified exceptions. Under FCRA, a consumer reporting agency may generally not provide a consumer report to an employer, or prospective employer, without the consumer’s written consent. A consumer reporting agency may not report medical information to creditors, insurers, or employers without the consumer’s permission. In addition, other consent requirements may apply under FCRA in various contexts.

b. Sensitive Data

GLBA does not include a classification of “sensitive” information, although collection of health or medical information may be subject to greater protection under state law implementation of GLBA in the insurance sector, and also may be subject to federal regulation in certain circumstances under other laws, such as the Health Insurance Portability and Accountability Act.

FCRA contains restrictions on collection, use, and disclosure of medical information and also contains special restrictions related to identity theft, consumer reports furnished for employment purposes, and a special category of consumer reports involving personal interviews with third parties termed “investigative consumer reports.”

c. Minors

GLBA does not specifically establish rules related to minors, although under general principles of contract law and regulatory requirements, minors might not be able to provide valid consent because of a lack of capacity to enter an enforceable contract.

FCRA does not specifically establish rules related to minors, although under general principles of contract law and regulatory requirements, minors might not be able to provide valid consent because of a lack of capacity to enter an enforceable contract.
d. Employee Consent

Under GLBA, where employees also qualify as consumers or customers, the same requirements regarding notice and opt-out consent apply equally to such individuals.

For FCRA, see Section 5(a) above.

e. Online/Electronic Consent

Under GLBA, the extent to which electronic notice and opt-out consent are sufficient depends upon applicable regulations and various factors, including whether the financial institution regularly conducts transactions with the consumer electronically.

For FCRA, the extent to which electronic notice and opt-out consent are sufficient depends upon applicable regulations and various factors, including whether the consumer agrees to engage in such transaction electronically.

6. Information/Notice Requirements

Generally, under GLBA, consumers are entitled to receive a privacy notice from a financial institution only if the company shares the consumers’ information with companies not affiliated with it, with some exceptions. Customers must receive a notice at the time the customer relationship is established and annually for every year during the continuation of the customer relationship. In 2014, however, the CFPB announced a finalized rule that enables certain financial institutions to comply with GLBA by publishing their privacy notices online instead of mailing them to their customers. This new rule only applies to financial institutions regulated by the CFPB, and does not impact those entities regulated by the Securities & Exchange Commission, Commodity Futures Trading Commission, Federal Trade Commission, or a state insurance regulator. The final rule requires the financial institution that wishes to rely on this alternative method of delivery to continuously post the annual privacy notice in a clear and conspicuous manner on a page of its website, without requiring a login or similar steps to access the notice. It allows financial institutions to use the alternative delivery method for annual privacy notices if:

- No opt-out rights are triggered by the financial institution’s information sharing practices under
- GLBA or the Fair Credit Reporting Act (“FCRA”) Section 603, and opt-out notices required by FCRA Section 624 have previously been provided, if applicable, or the annual privacy notice is not the only notice provided to satisfy those requirements;

• the information included in the privacy notice has not changed since the customer received the previous notice; and

• the financial institution uses the model form provided in Regulation P as its annual privacy notice.

Under FCRA, any user of a consumer report from a consumer reporting agency that takes an adverse action against a consumer based on the report – such as denying an application for credit, insurance, or employment – must notify the consumer of that fact, and give the consumer the name, address, and phone number of the consumer reporting agency that provided the consumer report. In addition, see Section 4(a) above for further requirements related to providing notice of opt-out rights in connection with sharing non-experience information among affiliates.

7. Processing Rules

In addition to the rules described above, other important provisions of GLBA also affect how a company conducts business. For example, financial institutions are prohibited from disclosing their customers’ account numbers to non-affiliated companies when it comes to telemarketing, direct mail marketing, or other marketing through e-mail, even if the individuals have not opted out of sharing the information for marketing purposes. Another provision prohibits “pretexting” – the practice of obtaining customer information from financial institutions under false pretenses.

Under FCRA, consumer reporting agencies, users of consumer reports, and furnisher of information to consumer reporting agencies are subject to a wide range of requirements with respect to the collection, use, and disclosure of this relevant information.

8. Rights of Individuals

a. Access Right

GLBA generally does not contain a right for the consumer to access and correct his or her non-public personal information.

Under FCRA, at the request of the consumer, a consumer reporting agency must provide the consumer with the information in his or her consumer report as well as a list of everyone who has requested it recently. There is generally no charge for the report if a user has taken an adverse action against the consumer because of information supplied by the consumer reporting agency. The consumer also is entitled to one free report every twelve months upon request in some instances, and has various rights to challenge the accuracy of information in his or her consumer report (as described below under “Additional Rights”).
b. Additional Rights

Consumers and customers have a wide range of other rights under applicable federal and state financial privacy regulations. For example, a significant additional right under FCRA and The Fair and Accurate Credit Transactions Act of 2003 relates to direct marketing. Specifically, when an organization markets to consumers based on information received from an affiliate, there may be a separate, additional notice and opportunity to opt-out of receiving such marketing.

With respect to consumer reporting agencies under FCRA, if a consumer tells a consumer reporting agency that his or her file contains inaccurate information, the consumer reporting agency must investigate the identified items (usually within 30 days) by providing the agency’s information source with all relevant evidence submitted by the consumer, unless the dispute is frivolous. The information source must review the submitted evidence and report its findings to the consumer reporting agency. (The information source also must advise national consumer reporting agencies to which it has provided the data of any error.) The consumer reporting agency must give the consumer a written report of the investigation, and also a copy of the consumer’s report if the investigation results in any change. If the consumer reporting agency’s investigation does not resolve the dispute, the consumer may add a brief statement to his or her file. The consumer reporting agency must normally include a summary of the statement in future reports. If an item is deleted or a dispute statement is filed, the consumer may ask that anyone who has recently received the report be notified of the change. A consumer reporting agency must remove or correct inaccurate or unverified information from its files, usually within 30 days after the consumer disputes it. However, the consumer reporting agency is not required to remove accurate data from the consumer’s file unless it is outdated (as described below) or cannot be verified. If the consumer’s dispute results in any change to the consumer’s report, the consumer reporting agency cannot reinsert the disputed item into the consumer’s file unless the information source verifies its accuracy and completeness. In addition, the consumer reporting agency must give the consumer a written notice telling the consumer that it has reinserted the item. The notice must include the name, address, and phone number of the information source. If the consumer tells anyone – such as a creditor who reports to a consumer reporting agency – that the consumer disputes an item, they may not then report the information to a consumer reporting agency without including a notice of the consumer’s dispute. In addition, once the consumer has notified the information source of the error in writing, it may not continue to report the information if it is, in fact, an error. In most cases, a consumer reporting agency may not report negative information that is more than seven years old; the term is ten years for bankruptcies. Creditors and insurers may use file information as the basis for sending a consumer unsolicited offers of credit or insurance. Such offers must include a toll free phone number for the consumer to call to remove the consumer’s name and
address from future lists. If the consumer calls, the consumer must be kept off the lists for two years. If the consumer requests, completes, and returns the consumer reporting agency form provided for this purpose, the consumer must be taken off the lists indefinitely.

9. Registration/Notification Requirements

GLBA contains no requirements to register with or notify regulatory authorities about data handling practices, although privacy and data security are often important components of regulatory oversight and audits.

FCRA does not generally establish registration requirements for a consumer reporting agency.

10. Data Protection Officers

For GLBA, see Section 12 below regarding security requirements.

FCRA does not generally establish requirements for a consumer reporting agency to appoint a chief privacy officer.

11. International Data Transfers

GLBA contains no express geographic restrictions on international data transfers, although the circumstances of the transfer must be taken into account when developing the security measures to be applied to the personal data, and regulators at both the federal and state level may impose oversight over the security of outsourcing and offshoring activities.3

FCRA contains no express geographic restrictions on international data transfers, although the circumstances of the transfer should be taken into account when a consumer reporting agency discloses a consumer report to a user.

12. Security Requirements

GLBA Interagency Guidelines establish requirements for financial institutions to protect the security of non-public personal information, including taking steps to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the financial institution’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each financial institution must:

- designate one or more employees to coordinate the safeguards;

• identify and assess the risks to customer information in each relevant area of the company’s operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
• design and implement a safeguards program, and regularly monitor and test it;
• select appropriate service providers and contract with them to implement safeguards; and
• evaluate and adjust the program in light of relevant circumstances, including changes in the firm’s business arrangements or operations, or the results of testing and monitoring of safeguards. Additional rules apply in the area of security breach notification and safe disposal of consumer information.

FCRA contains a wide range of data integrity and accuracy requirements, including those described above. Additional rules also apply to the safe disposal of information in or derived from consumer reports. In addition, pursuant to an amendment of the FCRA, the Federal Trade Commission’s Red Flag Rules (16 CFR Part 681) became effective. The rules require creditors that use consumer reports, furnish information to consumer credit reporting agencies, or advance funds to or on behalf of a person with certain covered accounts to develop and implement written identity theft prevention programs. The programs must provide for the identification, detection, and response to red flags that could indicate identity theft.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

GLBA establishes special rules for the protection, security and confidentiality of non-public personal information when disclosed to third party service providers.

FCRA generally does not specifically establish restrictions on the use of outsourcing providers, although case law contains some relevant requirements on the use of “agents,” and any organization should be aware of other applicable regulatory requirements as well as other general fiduciary obligations to maintain the integrity and security of information.

14. Enforcement and Sanctions

The CFPB, the federal banking agencies, other federal regulatory authorities, and state insurance authorities enforce GLBA with regard to entities within their authority. Each federal agency has issued substantially similar rules implementing GLBA’s privacy provisions. The states are responsible for issuing regulations and enforcing the law with respect to insurance providers.
In relation to FCRA, the CFPB generally has regulatory authority over consumer reporting agencies, and federal functional regulators generally have certain authority over financial institutions that are users of consumer reports or furnishers of information to consumer reporting agencies or that otherwise are regulated under FCRA. State attorneys-general have certain authority to pursue organizations for violations of FCRA, and aggrieved individuals can also pursue organizations in certain circumstances for violations of FCRA requirements.

15. Data Security Breach

a. Are there any legal requirements, including notification obligations, in the event of a data security breach?

While GLBA does not specifically impose notification obligations if a data security breach occurs, federal regulators have issued guidance on notification obligations on financial institutions when a data security breach occurs. Among other elements, this Guidance calls for financial institutions to notify their affected customers and primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information. In addition, GLBA requires financial institutions to ensure the security and confidentiality of customer information and to protect against unauthorized access or use of customer data that may result in harm to the customer. Under GLBA, financial institutions are required to establish a comprehensive information security program that includes appropriate incident response procedures. GLBA security guidelines generally provide that financial institutions must implement a program to address unauthorized access of customer data, including customer and authority notification, and mandate disclosure of a security breach if the financial institution determines that “misuse of its information about a customer has occurred or is reasonably possible.”

b. Risk of non-compliance

Violations of GLBA can result in various civil penalties and sanctions, including fines and other consequences that vary depending on the responsible regulatory authority.

Violations of FCRA can result in criminal and civil penalties. Civil penalties in the case of willful noncompliance can include up to $1,000 in statutory damages if no actual damages exist, actual damages, punitive damages, plus attorneys’ fees and costs.

16. Is there a filing requirement when a whistle-blower hotline is introduced in your jurisdiction?

No specific rules apply under GLBA or FCRA.

17. Would the implementation of an e-discovery system within an organization raise privacy issues?

Generally, yes, to the extent that the e-discovery system involves the collection, use, or disclosure of non-public personal information under GLBA, or consumer reports under FCRA, and utilizes third party service providers.

18. Would the introduction of a spam-filtering solution in an organization raise privacy issues?

Generally, yes, to the extent that the spam-filtering system involves the collection, use, or disclosure of non-public personal information under GLBA, or consumer reports under FCRA, and utilizes third party service providers.
United States Health Insurance Portability and Accountability Act

1. Recent Privacy Developments

The most recent significant developments to HIPAA/HITECH occurred in 2013. The Health Information Technology for Economic and Clinical Health Act, Sec. 13001 of the American Recovery and Reinvestment Act, Public Law 111-005 ("HITECH Act"), established important amendments to HIPAA (as defined below), including (i) mandatory notification in the event of a security breach; and (ii) direct application of certain information security and other HIPAA provisions, including the heightened penalty provisions, to an expanded range of organizations, such as (a) Business Associates of Covered Entities (which previously only needed to adhere to agreements with such Covered Entities), and (b) application of breach notification obligations to vendors of personal health records (previously not covered by HIPAA).

Since the enactment of HITECH, the Department of Health and Human Services ("HHS"), through the HHS Office for Civil Rights ("OCR"), had engaged in considerable rulemaking activity and increased its enforcement of HIPAA’s Privacy and Security Rules (discussed further below in Section 14). Then, after a number of delays, HHS released on 25 January 2013, the final omnibus rules codifying and modifying many of these interim rules, including those regarding heightened penalties, breach notification, and direct applicability to Business Associates (the “Final Rules”). The effective date of the Final Rules was 26 March 2013, and Covered Entities and Business Associates were required to be in compliance with the new requirements by 23 September 2013. Covered Entities and Business Associates have an additional year to conform existing BAAs to the requirements of the Final Rules, meaning this period will expire this year.

In part, the Final Rules:

- Confirm that Business Associates (as well as their subcontractors that access or receive Protected Health Information) are directly liable for compliance with certain of the requirements of the HIPAA Privacy and Security Rules and are subject to related penalties for violation of such requirements;
• Impose more stringent limitations on the use and disclosure of Protected Health Information for marketing and fundraising purposes as well as prohibitions on the sale of Protected Health Information without individual authorization;

• Require modifications to and redistribution of a Covered Entity’s Notice of Privacy Practices;

• Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools and to enable access to decedent information by family members or others;

• Increase individual rights of access to Protected Health Information by allowing patients to request a copy of their electronic medical record in electronic form and allowing individuals to instruct their providers not to share information about their treatment with their health plan if they pay in full for the relevant product or service;

• Adopt the increased and tiered civil money penalty structure provided by the HITECH Act (which was originally published as an interim final rule on 30 October 2009);

• Adopt the breach notification rule for Covered Entities and Business Associates and replace the “harm” threshold for notification with an evaluation regarding whether the breached data was “compromised”.

The Final Rules also include additional modifications related to the use and disclosure of genetic information.

Prior to the issuance of the Final Rules, HHS released on 31 May 2011, a notice of proposed rulemaking on the HIPAA accounting of disclosures requirement. The purpose was, in part, to implement the statutory mandate under HITECH to require Covered Entities and Business Associates to account for disclosures of Protected Health Information to carry out treatment, payment, and health care operations. Under the pre-HITECH rule, covered entities were not required to provide an accounting of disclosures for these types of uses and disclosures.

The proposed 2011 rules also, apparently based on HHS’s general authority under HIPAA, expanded the current accounting provision to provide individuals with the right to receive an access report detailing the internal access to Protected Health Information in a designated record set. If adopted in this form, these rules may pose challenges for Covered Entities that otherwise may be in the process of adopting electronic health records, as the detailed provisions regarding access tracking may not be contemplated by their current implementations. Comments for this proposed rule were accepted until 1 August 2011. The proposed May 2011 rules were not addressed in the Final Rules. HHS noted in the Final Rules, however, that these rules remain in effect and will be subject to additional rulemaking.
2. Emerging Privacy Issues and Trends

HITECH represents a significant expansion of federal law to protect health and medical privacy, and to protect individuals from medical identity theft. The adoption of the Final Rules, which contain more stringent penalties, obligations on Business Associates, and breach requirements as well as the related enforcement activity by HHS signals the on-going focus on this issue. In addition, with the increase in the number of high profile security breaches, special focus on the breach notification requirements seems likely. There will likely be attention paid to how and if cloud providers are subject to HIPAA (for example, as Business Associates).

3. Law Applicable

Standards for Privacy of Individually Identifiable Health Information issued pursuant to sections 1171 through 1179 of the Social Security Act ("HIPAA"), as added by sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and implemented in 45 C.F.R. Parts 160, 162 and 164 ("HIPAA Privacy Standards").

4. Scope of the Law

The regulations are applicable to the following entities, defined as “Covered Entities”:

- a health plan;
- a health care clearinghouse; and
- a health care provider that transmits any health information in electronic form in connection with a transaction covered by a HIPAA standard.

Certain portions of the regulations related to information security, breach notification, and other provisions are directly applicable to service providers of Covered Entities, defined as “Business Associates”; in addition, breach notification requirements apply to third party vendors of personal health records and certain other non-HIPAA covered entities.

a. Personal Data

The regulations govern the use and disclosure of “Protected Health Information”, which is individually identifiable health information, maintained in any format, that has been transmitted in an electronic format. Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

- is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

5. Consent Requirements
A Covered Entity may obtain consent of the individual to use or disclose Protected Health Information to carry out treatment, payment, or health care operations. A Covered Entity must obtain an individual’s authorization to use and disclose Protected Health Information for any purpose other than those permitted by the HIPAA Privacy Standards. The requirement to seek authorization for the use and disclosure of Protected Health Information for research may be waived with the approval of an Institutional Review Board or a privacy board appointed by the Covered Entity.

a. Authorization Content
A valid authorization must include the following elements:

- a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- if the information will be used for marketing purposes in exchange for financial remuneration from a third party, a statement to that effect;
- if information is to be sold, a statement that disclosure will result in remuneration to the Covered Entity;
- the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- the name or other specific identification of the person(s), or class of persons, to whom the Covered Entity may make the requested use or disclosure;
- a description of each purpose of the requested use or disclosure;
- an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure; and
- signature of the individual and date.

In addition, the authorization must contain statements adequate to place the individual on notice of all of the following:

- the individual’s right to revoke the authorization in writing, and either: (i) the exceptions to the right to revoke and a description of how the
individual may revoke the authorization; or (ii) a reference to the Covered Entity’s privacy notice;

- the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either: (i) the Covered Entity may not condition treatment, payment, enrolment or eligibility for benefits on whether the individual signs the authorization; or (ii) the consequences to the individual of a refusal to sign the authorization when the Covered Entity may, in compliance with HIPAA, condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization;

- the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by HIPAA.

The authorization must be written in plain language, and certain restrictions apply with regard to compound authorizations. If a Covered Entity seeks an authorization from an individual for a use or disclosure of Protected Health Information, the Covered Entity must provide the individual with a copy of the signed authorization.

6. Information/Notice Requirements

A Covered Entity must provide a notice that is written in plain language and that contains the following elements:

- a header;

- a description, including at least one example, of the types of uses and disclosures that the Covered Entity is permitted to make for each of the following purposes: treatment, payment, and health care operations;

- a description of each of the other purposes for which the Covered Entity is permitted or required to use or disclose Protected Health Information without the individual’s written authorization;

- a description of any applicable legal limitation more stringent than the HIPAA Privacy Standards on the uses or disclosure of Protected Health Information;

- if applicable, a statement that the Covered Entity may contact the individual to raise funds for the Covered Entity and that the individual has the right to opt out of receiving such communications;

- if applicable, that a group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan;
• notice of the right to request restrictions on certain uses and disclosures of Protected Health Information, including a statement that the Covered Entity is not required to agree to a requested restriction (except where an individual requests a restriction on disclosure to a health plan for a product or service for which payment has been made in full);

• notice of the right to receive confidential communications of Protected Health Information;

• notice of the right to inspect and copy Protected Health Information;

• notice of the right to amend Protected Health Information;

• notice of the right to receive an accounting of disclosures of Protected Health Information;

• notice of the right to obtain a paper copy of the notice from the Covered Entity upon request;

• a statement that the Covered Entity is required by law to maintain the privacy of Protected Health Information and to provide individuals with notice of its legal duties and privacy practices with respect to Protected Health Information and to notify individuals following a breach of unsecured Protected Health Information;

• a statement that the Covered Entity is required to abide by the terms of the notice currently in effect;

• a statement that the Covered Entity reserves the right to change the terms of its notice and to make the new notice provisions effective for all Protected Health Information that it maintains (the statement must also describe how the Covered Entity will provide individuals with a revised notice);

• a statement that individuals may complain to the Covered Entity and to HHS if they believe their privacy rights have been violated;

• the name, or title, and telephone number of a person or office to contact for further information; and

• the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

The Covered Entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual’s rights, the Covered Entity’s legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected. A covered health plan must distribute
its privacy notice at least once every three years to all then current participants.

7. Rights of Individuals

a. Access Right
An individual has a general right of access to inspect and obtain a copy of Protected Health Information about the individual in a designated record set, for as long as the Protected Health Information is maintained in the designated record set. A designated record set is broadly defined as a set of records on which a Covered Entity may make decisions about an individual.

As noted above, the 11 May 2011 proposed rules in their current form expand such access rights. Moreover, the Final Rules provide specific additional rights to request information in a particular form.

b. Accounting of Disclosure Rights
An individual has a right to receive an accounting of disclosures of Protected Health Information made by a Covered Entity in the six years prior to the date on which the accounting is requested, except for disclosures:

- to carry out treatment, payment and health care operations;
- to individuals of Protected Health Information about them;
- incident to a use or disclosure otherwise permitted or required;
- pursuant to an authorization;
- for the facility’s directory or to persons involved in the individual’s care or other notification purposes;
- for national security or intelligence purposes;
- to correctional institutions or law enforcement officials;
- as part of a limited data set; or
- that occurred prior to the compliance date.

As noted above, the 11 May 2011 rules in their current form expand the situations for which Covered Entities must provide an accounting of disclosures of Protected Health Information.

c. Amendment Rights
A Covered Entity must permit an individual to request that the Covered Entity amend the Protected Health Information maintained in the designated record set. The Covered Entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested
amendment, provided that it informs individuals in advance of such requirements.

d. Right to Restrict Uses and Disclosures
A Covered Entity must allow an individual to request restrictions on the uses and disclosures of Protected Health Information about the individual. A Covered Entity needs not to agree to a requested restriction, but must abide by any agreed upon restriction except in the event that the information is required to provide emergency treatment to the individual. Under the Final Rules, individuals have the right to instruct their provider not to share information about their treatment with their health plan if they pay in full for the relevant product or service.

e. Right to Request Confidential Communications
A health care provider must accommodate reasonable requests from individuals to receive communications by alternate means or locations. A health plan must accommodate reasonable requests for such confidential communications when the individual states that the basis for the request is that the disclosure of Protected Health Information could endanger the individual.

8. Privacy Officer
A Covered Entity must appoint a privacy officer who is generally responsible for the implementation and enforcement of policies and practices of the Covered Entity required by the HIPAA Privacy Standards.

9. International Data Transfers
There are no specific requirements within the regulations applicable to international transfers of data. A Covered Entity is required to comply with the requirements of HIPAA with respect to data that has been transferred outside of the US.

10. Data Retention Obligations
Covered Entities are required to maintain all documents required under these regulations for six years.

11. Security Requirements
Covered Entities and Business Associates must comply with the Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Parts 160 and 164. The application of many of the Security Standards to Business Associates was re-confirmed in the Final Rules.
12. Requirements Applicable to Employer-Sponsored Health Plans

An employer plan sponsor who requires access to Protected Health Information other than summary health information or enrollment/disenrollment information must certify to the plan that the plan documents have been amended to incorporate provisions required by the HIPAA Privacy Standards before the plan may disclose Protected Health Information to the employer plan sponsor. The plan amendment must provide that the employer plan sponsor will:

- not use or further disclose the information other than as permitted or required by the plan documents or as required by law;
- ensure that any agents, including a subcontractor, to whom it provides Protected Health Information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;
- not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;
- report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;
- make available Protected Health Information, as required by the HIPAA Privacy Standards;
- make available Protected Health Information for amendment and incorporate any amendments to Protected Health Information in accordance with the HIPAA Privacy Standards;
- make available the information required to provide an accounting of disclosures in accordance with the HIPAA Privacy Standards;
- make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from the group health plan available to HHS for purposes of determining compliance by the group health plan with the HIPAA Privacy Standards;
- if feasible, return or destroy all Protected Health Information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible;
• describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the Protected Health Information to be disclosed, provided that any employee or person who receives Protected Health Information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

• restrict the access to and use by such employees to plan administration functions that the plan sponsor performs for the group health plan; and

• provide an effective mechanism for resolving any issues of noncompliance with plan document provisions.

13. Requirements Applicable to Outsourcing or Transfer to Third Parties

Generally, disclosures of Protected Health Information to third parties can only be made pursuant to a valid authorization from each individual whose Protected Health Information is being disclosed. Subject to the conditions described below, a Covered Entity may disclose Protected Health Information without prior authorization to Business Associates, which are third parties that:

• on behalf of the Covered Entity, assist in the performance of: (i) a function or activity involving the use or disclosure of individually identifiable health information; or (ii) any other function or activity regulated by standards promulgated pursuant to the HIPAA statute; or

• provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a Covered Entity, where the provision of the service involves the disclosure of Protected Health Information from the Covered Entity, or from another Business Associate of such Covered Entity, to the Business Associate. A Covered Entity may disclose Protected Health Information to a Business Associate and may allow a Business Associate to create or receive Protected Health Information on its behalf, if the Covered Entity obtains satisfactory assurance that the Business Associate will appropriately safeguard the information.

Business Associate also includes: A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to Protected Health Information to a Covered Entity and that requires access on a routine basis to such Protected Health Information; a person that offers a personal health record to one or more individuals on behalf of a Covered Entity; and a subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of a Business Associate.
In particular, the Covered Entity must enter into a contract with the Business Associate that:

- establishes the permitted and required uses and disclosures of Protected Health Information by the Business Associate;

- prohibits the Business Associate to use or further disclose the information in a manner that would violate the requirements of HIPAA, if done by the Covered Entity, except that: (i) the contract may permit the Business Associate to use and disclose Protected Health Information for the proper management and administration of the Business Associate; and (ii) the contract may permit the Business Associate to provide data aggregation services relating to the health care operations of the Covered Entity;

- provides that the Business Associate will: (i) not use or further disclose the information other than as permitted or required by the contract or as required by law; (ii) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract; (iii) report to the Covered Entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including any breaches of unsecured Protected Health Information; (iv) ensure that any agents, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by the Business Associate on behalf of, the Covered Entity agrees to the same restrictions and conditions that apply to the Business Associate with respect to such information; (v) make available Protected Health Information in accordance with the HIPAA Privacy Standards; (vi) make available Protected Health Information for amendment and incorporate any amendments to Protected Health Information in accordance with the HIPAA Privacy Standards; (vii) make available the information required to provide an accounting of disclosures in accordance with the HIPAA Privacy Standards; (viii) to the extent the Business Associate is to carry out a Covered Entity’s obligation under the HIPAA Privacy Standards, comply with the requirements of the Privacy Standards that apply to the Covered Entity in the performance of such obligation; (ix) make its internal practices, books, and records relating to the use and disclosure of Protected Health information received from, or created or received by the Business Associate on behalf of, the Covered Entity available to the US government (Secretary of HHS) for purposes of determining the Covered Entity’s compliance with HIPAA; and (x) at termination of the contract, if feasible, return or destroy all Protected Health Information received from, or created or received by the Business Associate on behalf of, the Covered Entity that the Business Associate maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible;
authorizes termination of the contract by the Covered Entity, if the Covered Entity determines that the Business Associate has violated a material term of the contract;

In addition, the contract may permit the Business Associate to use the information received by the Business Associate in its capacity as a Business Associate to the Covered Entity, if necessary: (i) for the proper management and administration of the Business Associate; or (ii) to carry out the legal responsibilities of the Business Associate; and the Business Associate may be permitted to disclose the information received by the Business Associate in its capacity as a Business Associate, if: (i) the disclosure is required by law; or (ii) the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

A Covered Entity is not in compliance with the HIPAA Privacy Standards if the Covered Entity knows of a pattern of activity or practice of the Business Associate that constituted a material breach or violation of the Business Associate’s obligation under the contract or other arrangement, unless the Covered Entity takes reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminate the contract or arrangement, if feasible. The same obligation applies to Business Associates with regard to downstream subcontractors.

Additionally, pursuant to the HIPAA Security Standards, a Business Associate must agree to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, availability and integrity of electronic Protected Health Information that is created, received, maintained or stored on behalf of a Covered Entity. The Business Associate must report any security incident to the Covered Entity of which it becomes aware. In addition, as noted above, the Business Associate must ensure that its agreement with any subcontractor includes a requirement that these safeguards be implemented as well.

Under the Final Rules, Covered Entities have until September 2014 to make sure that existing Business Associate Agreements conform to the new requirements for Business Associate Agreements.

14. Enforcement and Sanctions

HHS may impose a civil money penalty on any person who violates the HIPAA Privacy Standards in the range from $100 to $50,000 per violation, with a total of $25,000 to $1.5 million for all violations of a single requirement in a calendar year. Violations of the HIPAA Privacy Standards can also carry criminal penalties, including up to ten years imprisonment in certain cases.
Under HITECH, such penalties may now be imposed on Business Associates as well as Covered Entities.

Over the course of the year, HHS continued to demonstrate a heightened interest in enforcing HIPAA and imposed additional civil money penalties on entities for violations of the HIPAA Privacy and Security Rules.

15. Data Security Breach

a. Are there any legal requirements, including notification obligations, in the event of a data security breach?

The HITECH Act amended HIPAA to include a security breach notification requirement. These notification requirements apply in the event of a breach of unsecured Protected Health Information, which generally means Protected Health Information that is not secured by technology (e.g., encryption) that makes it unreadable, unusable or indecipherable to unauthorized individuals. A “breach” is presumed to have occurred if there is an acquisition, access, use or disclosure of Protected Health Information in a manner not permitted by the Privacy Rule unless a risk assessment determines a “low probability” that the breached data were compromised. The four factors that risk assessments must consider are:

1. the nature and extent of the Protected Health Information involved, including the likelihood data could be reidentified;
2. the unauthorized person who used Protected Health Information or to whom an improper disclosure was made;
3. whether the Protected Health Information was actually acquired or viewed; and
4. the extent to which the risk to the Protected Health Information was mitigated.

Several features of the notification requirement include:

- obligations for the Covered Entity to notify affected individuals upon discovery of a breach (and in no case later than 60 days after such discovery or after such breach should have reasonably been discovered);
- obligations for Business Associates to notify the relevant Covered Entity upon discovery of a breach;
- definitions for key terms, such as: “discovery” of breach; “unsecured protected health information” (i.e., the type of data subject to the notification requirement); and “timeliness” of transmitting the notification;
- obligations to transmit the notice to affected individuals in writing or other specified means;
• if more than 500 individuals are affected, mandatory obligations to notify media;
• obligations to notify the HHS of all breaches (if 500 or more individuals are affected, such notification must be made at the time of the notification to the affected individuals; if fewer than 500 individuals are affected, such notification must be made at the end of the calendar year);
• content requirements for notices (e.g., date of breach, date of discovery, data compromised, and the like); and
• other specific obligations.

Additional breach notification duties apply to vendors of personal health records, as per the Health Breach Notification Rule adopted by the Federal Trade Commission (16 CFR Part 318).

b. Risk of non-compliance

Failure to comply with the breach notification requirements constitutes a violation of HIPAA that can be subject to the penalties described in Section 14 above.

16. Is there a filing requirement when a whistle-blower hotline is introduced in your jurisdiction?

No.

17. Would the implementation of an e-discovery system within an organization raise privacy issues?

Under the HIPAA Privacy Standards, a Covered Entity may disclose Protected Health Information in accordance with applicable laws, including in response to lawful discovery requests or subpoenas where the parties have sought a qualified protective order from the court or that the subject of the information being requested has received notice of the discovery request or subpoena. In order to provide Protected Health Information to vendors in the event of litigation, a Business Associate Agreement may be required.

18. Would the introduction of a spam-filtering solution in an organization raise privacy issues?

The HIPAA Privacy and Security Standards do not have requirements directly addressing this topic. Under HIPAA, a Covered Entity would need to ensure that a spam-filtering solution: (a) does not result in a disclosure of Protected Health Information in a manner not permitted by HIPAA; and (b) does not interfere with the confidentiality, integrity, or availability of electronic Protected Health Information.
United States State Data Security Laws

1. Recent Developments and Trends

A growing number of US states have enacted laws requiring entities that possess certain categories of personal information to implement reasonable security requirements. Such laws generally apply to any entity that owns or licenses certain categories of personal information about a resident of the state that has promulgated such laws. Certain US states, such as Massachusetts and Oregon, have promulgated fairly specific requirements for the protection of personal information. For example, the Massachusetts’s Office of Consumer Affairs and Business Regulation has promulgated data security regulations pursuant to Chapter 93H of the General Laws of Massachusetts. The Massachusetts regulations differ from other US state data security laws in that they require covered entities to implement a number of specific administrative, physical, and technical safeguards on a comprehensive level, rather than articulating a reasonableness standard or establishing certain data security measures for particular data fields (e.g., Social Security Number). Other states may find the regulations influential in interpreting or making law, as shown by a large volume of pending state bills on data security. For example, in 2014 the New York legislature proposed a bill which if passed, would require any entity doing business in the state to implement a comprehensive information security program. The broad scope of the Massachusetts regulations and similar state data security laws in the future, will likely cover many entities that participate in interstate commerce but are outside of a state that has enacted such laws, since such entities typically process personal information of individuals from many states.

2. Laws Applicable

Massachusetts Gen. Laws (“MGL”) 93H, §§ 1-6 and Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR § 17.00 et seq., as amended on 12 February 2009 (hereinafter, the “Massachusetts Regulations”). See also Oregon Rev. Stat. § 646A.622 as another example of a US state law with specific data security requirements.

3. Key Privacy Concepts

a. Personal Data

“Personal information” is defined as “a Massachusetts resident’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social
Security number; (b) driver’s license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account; provided, however, that ‘Personal information’ shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."

b. Data Processing
The Massachusetts Regulations apply to persons that “own, license, store or maintain” personal information about a resident of the Commonwealth of Massachusetts, regardless of the medium in which such information is recorded or preserved (e.g., paper or electronic records).

c. Processing by Data Controllers
A covered entity may include “a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.”

d. Jurisdiction/Territoriality
The Massachusetts Regulations apply on their face to persons that “own, license, store or maintain” personal information about a resident of the Commonwealth of Massachusetts. Accordingly, the Massachusetts Regulations may have extra-jurisdictional effect on entities located outside of Massachusetts if they process personal information on Massachusetts residents.

e. Sensitive Personal Data
The Massachusetts Regulations do not distinguish between sensitive personal information and non-sensitive personal information.

f. Employee Personal Data
While the Massachusetts Regulations were primarily promulgated to protect consumers from identity theft, on their face, they can potentially apply to personal information of covered entities’ employees as well.

4. Processing Rules
“Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information. Such comprehensive information security program shall be reasonably consistent with industry standards, and shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records.”
following safeguards must be included, although, others not listed here are required as well:

- identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks;

- developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises;

- imposing disciplinary measures for violations of the comprehensive information security program rules;

- preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records;

- limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected;

- limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements;

- identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information;

- reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers;

- regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information, and upgrading information safeguards as necessary to limit risks;

- reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and
• documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

5. Data Protection Officers

Every comprehensive information security program must include the designation of at least one employee to maintain it.

6. International Data Transfers

A covered entity is required to comply with the regulations’ requirements with respect to personal information that has been transferred outside of the United States. There are, however, no specific requirements in the Massachusetts Regulations that are relevant to international transfers of data.

7. Security Requirements

Every covered entity that electronically stores or transmits personal information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, have the following elements:

• secure user authentication protocols;
• secure access control measures;
• encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly;
• reasonable monitoring of systems, for unauthorized use of or access to personal information;
• encryption of all personal information stored on laptops or other portable devices;
• reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of personal information in files on a system that is connected to the internet;
• reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions; and
• education and training of employees on the proper use of the computer security system and the importance of personal information security.
8. Special Rules for the Outsourcing of Data Processing to Third Parties

Every comprehensive information security program must include taking all reasonable steps to (i) verify that any third party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in the Massachusetts Regulations, and (ii) ensure that such third party service provider is applying security measures to personal information that are at least as stringent as those required under the Massachusetts Regulations.

9. Enforcement and Sanctions

Since 2011, the Massachusetts Attorney General has brought enforcement actions against companies that have violated the Massachusetts Regulations by failing to protect personal information in connection with data security breaches. For example, in 2012, the Massachusetts Attorney General announced that a Massachusetts hospital agreed to pay $750,000 to resolve allegations that the hospital failed to protect the personal and confidential health information of more than 800,000 consumers when hundreds of computer back-up tapes were lost in transit to an off-site location to be erased. In 2013, the Mass. AG announced that former owners of a medical billing practice agreed to collectively pay $140,000, settling allegations that sensitive medical records and confidential billing information for tens of thousands of Massachusetts patients were improperly disposed of at a public dump. In 2014, the Massachusetts Attorney General announced that a nationally chartered bank agreed to pay $825,000 to resolve allegations that it lost unencrypted personal information of more than 90,000 consumers when two back-up tapes were lost in transit by a third-party courier and that the bank delayed notifying the Massachusetts Attorney General and impacted consumers. As part of the settlement, the bank was also required to take steps to strengthen its security practices.

10. Data Security Breach

a. Are there any legal requirements, including notification obligations, in the event of a data security breach?

Data breach notification obligations are set forth in MGL 93H §3.

b. Risk of non-compliance

The Massachusetts Attorney General may bring an action pursuant to its statutory authority to remedy violations of the law. A Massachusetts court may issue injunctions and make such other orders or judgments as may be necessary to compensate injured parties. In addition, Massachusetts law provides for a civil penalty of $5,000 for each violation and may require the violator to pay the reasonable costs of investigation and litigation of such violation, including reasonable attorneys’ fees. Other states with data security...
laws provide for civil penalties of up to $1,000 per violation and up to $750,000 in the aggregate for continuing violations.
United States
State Security Breach Notification Laws

1. Recent Developments and Trends
As of January 2014, forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted notification laws involving security breaches of personal information. Generally, US state data breach notification laws apply to any entity that owns or licenses certain categories of personal information about a resident of the state that has promulgated such a law. Alabama, Kentucky, New Mexico and South Dakota do not have security breach notification laws. In 2013, the state of North Dakota expanded the scope of personal data subject to data breach notification to include medical and health insurance information, and the state of California expanded the scope of personal data subject to breach notification to include a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

2. Law Applicable
This summary will focus on California’s security breach notification law, Cal. Civ. Code § 1798.82, the first such law in the United States. Accordingly, although other state laws’ requirements and scope differ from those of California, most state laws follow the basic principles of Cal. Civ. Code § 1798.82.

No generally applicable federal law on security breach notification has been enacted to date, but the federal Health Insurance Portability and Accountability Act also contains certain security breach notification requirements, which were introduced by the Health Information Technology for Economic and Clinical Health Act (see summary on HIPAA). The Gramm-Leach-Bliley Act also establishes breach notification requirements that apply to financial institutions (see summary on GLBA/FCRA).

3. Key Privacy Concepts

a. Personal Data
“Personal information” means (1) an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (a) Social Security number, (b) Driver’s license number or California Identification Card number, (c) Account number, credit or debit card number, in combination with
any required security code, access code, or password that would permit access to an individual's financial account, (d) Medical information, (e) Health insurance information; or (2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

“Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

“Medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. “Health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.

Note that state breach notification requirements outside of California can often have a broader scope and apply to name in combination with additional data fields, such as (a) Date of birth; (b) Mother’s maiden name; (c) Digitized or electronic signature; (d) Unique electronic identifier or routing code, in combination with any access code or password that would permit access to a financial account; (e) Passwords; and (f) Identification number assigned to an individual by the individual’s employer.

b. Processing by Data Controllers
Covered entities include any person or business that conducts business in California and that owns or licenses computerized data that includes personal information.

c. Sensitive Personal Data
Cal. Civ. Code § 1798.82 does not distinguish between sensitive and non-sensitive personal information.

d. Employee Personal Data
Notice obligations under Cal. Civ. Code § 1798.82 do not distinguish between types of data subjects, e.g., customers or employees. However, only customers of a covered business are eligible to recover damages for violations of Cal. Civ. Code § 1798.82.

4. Information/Notice Requirements
Cal. Civ. Code § 1798.82 requires that that data breach notice meet certain content requirements, as follows:

(1) The security breach notification shall be written in plain language.
(2) The security breach notification shall include, at a minimum, the following information: (A) The name and contact information of the reporting person or business subject to this section. (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach. (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice. (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided. (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided. (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver’s license or California identification card number.

(3) At the discretion of the person or business, the security breach notification may also include any of the following: (A) Information about what the person or business has done to protect individuals whose information has been breached. (B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(4) In the case of a breach of the security of the system involving a “user name or email address, in combination with a password or security question and answer that would permit access to an online account” (and no other categories of personal information described by the statute), the person or business may (except in certain circumstances described by the statute) comply with the notification requirements by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

5. Rights of Individuals

Any customer injured may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated the law may also be enjoined.
6. Registration/Notification Requirements

Like many other US State laws, Cal. Civ. Code § 1798.82 now requires notification to the State’s Attorney General in certain circumstances. Specifically, Cal. Civ. Code § 1798.82 requires notification to the State’s Attorney General if a person or business subject to the law is required to notify more than 500 California residents.

7. Data Protection Officers

There are no requirements to appoint a data protection officer under Cal. Civ. Code § 1798.82.

8. Security Requirements

A separate California Civil Code provision (Cal. Civ. Code § 1798.81.5) requires a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

9. Special Rules for the Outsourcing of Data Processing to Third Parties

A separate California Civil Code provision (Cal. Civ. Code § 1798.81.5) requires a business, which discloses personal information about a California resident to a nonaffiliated third party, to require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

10. Enforcement and Sanctions

On July 19, 2012, the California Attorney General announced the creation of the Privacy Enforcement and Protection Unit in the California Department of Justice (“Privacy Unit”) which will focus on protecting consumer and individual privacy through civil prosecution of state privacy laws. Specifically, the Privacy Unit will enforce laws regulating the collection, retention, disclosure, and destruction of private or sensitive information by individuals, organizations, and the government.

11. Data Security Breach

Are there any legal requirements, including notification obligations, in the event of a data security breach?
Covered entities must disclose any “breach of the security of the system” following discovery or notification of the breach to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

“Breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

Any person or business that maintains computerized data that includes personal information that the person or business does not own must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Notice may be provided by one of several methods, including written notice, electronic notice, substitute notice, email notice, a website posting, and notification to major state-wide media.

Risk of non-compliance

The California data breach notification statutes provide for injunctions and private rights of action for California residents. Under US state breach notification laws generally, the penalties for non-compliance typically range from injunctions, civil penalties, and private rights of action. Civil penalties can range from $100 to $750,000 per violation. For continuing violations, civil penalties can be much larger.
Uruguay

Stephania Bresque
Montevideo
Tel: +598 2900 1000 ext. 1531
sbresque@ferrere.com

Martin Pesce
Montevideo
Tel: +598 2900 1000 ext. 1200
mpesce@ferrere.com
1. Recent Privacy Developments

In Uruguay, personal data protection is regulated under Law 18,331 and its Regulatory Decree 414/009. In August 2012, Uruguay was granted the adequacy note for international transfer purposes by the European Commission as the aforementioned regulation has been deemed aligned with European regulatory standards.

Furthermore, on 12 April 2013, the Council of Europe announced that Uruguay became the first non-European country to accede to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) and its Additional Protocol 3.3 The approval makes Uruguay the 45th country to be party to the Convention, which was included within the internal Uruguayan legal framework through Law 19,030 in November 2011.

2. Emerging Privacy Issues and Trends

- **Cloud computing**: This emerging technology is gaining popularity among multinational companies especially as it is seen to improve productivity and lower costs. The local Data Protection Authority has participated and hosted several events aimed at analyzing the risks involved in the implementation of cloud computing. The main issue of concern has been the fact that most cloud computing providers do not disclose the specific place where customer data will be held. This scenario implies a certain degree of risk for companies and becomes an issue in terms of ensuring compliance with local data protection regulation, which prohibits personal data transfers towards certain countries.

- **Bring Your Own Device (“BYOD”)**: Many companies have started to shift to a BYOD system. One of the issues when implementing a BYOD system is whether and to what extent the employer is entitled to monitor and control the use of such devices by their employees during work hours and personal time, as an exercise of the employer’s right of control. The local Data Protection Authority has yet to issue an opinion on the subject, and has yet to define the parameters within which said monitoring may be put in place when employees are using their own devices.

- **Cybercrime/Cybersecurity**: In 2014, the Executive Branch filed before the Legislative Branch a bill in order to regulate and sanction cybercrimes. The bill is currently under analysis in the Parliament, and it classifies the following as felonies: unauthorized access to a computer system; computer damage; computer fraud; phishing; personal data treatment through deceitful, abusive or extortive means.
3. Law Applicable

In Uruguay, the legal framework concerning personal data protection is rather new, and consists of two main regulations (the “Law”):

- Law No. 18,331 on Personal Data Protection and Habeas Data Action¹ (as amended by Laws No. 18,719 and 18,996), which was adopted on August 6, 2008

- Decree No. 414/009², which regulates the aforementioned law (as amended by Decree 308/014) enacted on August 31st, 2009

The aforementioned regulation was patterned after the European Directive 95/46 EC, accordingly it follows the European protective parameters. Both the Law and the Decree seek to protect the privacy of individuals and legal entities whose records are kept in databases.

The Law introduces several principles that ought to be complied with when collecting and processing personal data:

i. **Principle of Legality**: the formation of a database will be lawful when the database is properly registered. Moreover, a database cannot have purposes that infringe human rights or are contrary to law or public morals.

ii. **Principle of truthfulness/veracity**: Personal data collected for the purpose of processing shall be truthful, adequate, impartial and not excessive regarding the purpose for which it was obtained. Data collection shall not be carried out through unfair, fraudulent, abusive, extorsive means or in any way contrary to the provisions of the Law. Data shall be accurate and updated, if necessary. Whenever the inaccuracy or falseness of data is verified, the controller, as soon as he/she/it becomes aware of said circumstance, shall delete, complete or replace them with the accurate, truthful and updated data. Furthermore, out of date data shall be deleted.

iii. **Purpose Limitation Principle**: Data that is the object of processing shall not be used for purposes other than or incompatible with those motivating their collection. Data shall be deleted whenever they cease to be necessary or relevant for the purposes for which they were collected. The regulations shall determine cases and procedures in which, exceptionally,

---

¹ [http://datospersonales.gub.uy/wps/wcm/connect/829161004d0a999d861fcefd6066fd91/Descargar+Ley+N%C2%B0+18.331.pdf?MOD=AJPERES&amp;CONVERT_TO=url&amp;CACHEID=829161004d0a999d861fcefd6066fd91](http://datospersonales.gub.uy/wps/wcm/connect/829161004d0a999d861fcefd6066fd91/Descargar+Ley+N%C2%B0+18.331.pdf?MOD=AJPERES&amp;CONVERT_TO=url&amp;CACHEID=829161004d0a999d861fcefd6066fd91)

² [http://datospersonales.gub.uy/wps/wcm/connect/11c874804d1a397b9d83dffd6066fd91/Descargar+Decreto-414-009.pdf?MOD=AJPERES&amp;CONVERT_TO=url&amp;CACHEID=11c874804d1a397b9d83dffd6066fd91](http://datospersonales.gub.uy/wps/wcm/connect/11c874804d1a397b9d83dffd6066fd91/Descargar+Decreto-414-009.pdf?MOD=AJPERES&amp;CONVERT_TO=url&amp;CACHEID=11c874804d1a397b9d83dffd6066fd91)
and considering historical, statistical or scientific values, and according to specific legislation, personal data shall be kept even when said need or appropriateness has expired. Data shall not be communicated between databases, without it being stated by law or without the prior informed consent of the data subject.

iv. **Principle of prior consent:** Personal data processing shall be legal whenever the data subject has given his/her prior free, express and informed consent, which has to be documented, save for the exceptions detailed below.

v. **Principle of data security:** data controller or user of the database must take the necessary steps to ensure the security and confidentiality of personal data. Such measures must prevent the alteration, loss, consultation or unauthorized data treatment, as well as detect any re-direction of information, intentional or not, whether the risks come from human action or from the technical means used.

vi. **Principle of confidentiality:** Those natural or legal persons that lawfully obtain information from a database providing processing, are obliged to use it by keeping it confidential and exclusively for the usual operations of their business or activity; any dissemination of said information to third parties is prohibited. People who, due to their labor situation or other type of relationship with the data controller, have access or take part in any stage of personal data processing, are bound to protect the secrecy of data (article 302 of the Criminal Code), whenever collected from non-publicly-accessible sources. The above shall not apply in cases where there is an order by a competent justice, according to regulations in force on this subject or upon the data subject’s consent. This obligation shall prevail even after the relationship with the data controller has ended.

vii. **Principle of liability:** The data controller shall be liable for the non-compliance of the provisions stated in the Law.

4. **Key Privacy Concepts**

a. **Personal Data**

**Personal Data:** any kind of information regarding identified or identifiable natural or legal persons.

b. **Data Processing**

**Data Processing:** systematic procedures and operations, whether or not by automated means, allowing the processing of personal data, as well as their assignment to third parties through communications, queries, interconnections or transfers.
c. Processing by Data Controllers

Processing by Data Controllers: The Privacy Act applies to entities that undertake any of the acts or practices covered by the Law. No distinction is made between entities that are data controllers and those that are mere data processors treating the data on behalf of other entities. The only difference is on the degree of liability of the processing party, depending on whether the entity is a data controller or a data processor.

d. Jurisdiction/Territoriality

Jurisdiction/Territoriality: Personal data treatment/processing is subject to the Law in the following cases:

- The processing is being carried out by a data controller established within Uruguayan territory, the latter being the place where processing takes place.

- When the data controller is not established within Uruguayan territory but uses means located in the country for the processing of the data. An exception to this rule is that the aforementioned means are used exclusively for transit purposes, as long as the data controller designates a representative before the local Data Protection Authority, with address and permanent residency in Uruguay, in order to comply with its legal obligations. Such designation will not impede the initiation of legal actions against the data controller, nor will it diminish its liability as to the compliance of its obligations under the Law and the Decree.

Although the local Data Protection Authority has not yet clearly defined what “means” would include, it is likely to follow the Spanish Regulator’s criteria, which is broad and includes among the term “means” any type of device or tool (e.g., PCs, cookies, etc.).

e. Sensitive Personal Data

Sensitive Personal Data: personal data revealing racial or ethnic origin, political preferences, religious and moral beliefs, trade union membership and information regarding health or sex life.

f. Employee Personal Data

Employee Personal Data: local regulation does not provide a definition of “employee personal data”. Notwithstanding the foregoing, please note that, under the Law, personal data that is derived from a contractual, scientific, or professional relationship with the data subject, and is necessary for the development or fulfilment of such relationship (such being the case of employee personal data) is exempted from the prior consent requirement for its collection and treatment.
5. Consent

a. General

As a general rule, the data subjects’ free, prior, explicit and informed consent has to be obtained and the same must be documented prior to the collection and processing of personal data.

There are exceptions to the aforementioned principle. As such, prior consent shall not be necessary when:

- the data comes from public sources of information, such as registries or publications in mass media;
- the data is collected for the implementation of typical functions of the State powers or on account of a legal obligation;
- it involves lists whose data regarding natural persons are only limited to names and surnames, identity card number, nationality, address and date of birth. In the case of legal entities, corporate name, fancy name, Tax Payer Number, address, phone number and identity of the people in charge;
- the data derives from a contractual, scientific or professional relationship with the data subject, and is necessary for its development or execution;
- the processing is carried out by a natural person for his exclusive personal or household use.

For the consent to be considered informed, the law mandates the following information to be provided to the data subject:

- The purpose for which data shall be processed and who may be the recipients or categories of recipients of the data.
- The existence of the corresponding database, whether electronic or any other type, and the identity and address of the data controller.
- Whether replies to the proposed questionnaire are mandatory or voluntary, particularly regarding sensitive data.
- Consequences of the provision of data and of the refusal to do so, or their inaccuracy.
- The data subject’s possibility of exercising his/her rights of access rectification and deletion of his/her data.
b. Sensitive Data
The Law requires that sensitive data may only be processed with the express written consent of the data subject. Furthermore, sensitive data may only be collected and processed for reasons of public interest which are specifically provided in the Law.

Sensitive data can only be collected and can be subject to processing for reasons of general interest authorized by law, or when the requesting body has the legal order to do so. Moreover, these data can also be processed for statistical or scientific purposes when dissociated from the holders.

The formation of databases which store information that directly or indirectly discloses sensitive data are prohibited, except for those belonging to political parties, trade unions, churches, religious beliefs, associations, foundations and other non-profit entities with political, religious, philosophical or trade union, making reference to the racial or ethnic origin, health and sex life, regarding the data of their members or partners. In any case, the communication of said data shall always require the data subject’s previous consent.

c. Minors
Minors need their parents or tutor’s consents since the law indicates that they cannot express valid consent. In Uruguay, the age of majority is 18.

d. Employee Consent
The local Data Protection Authority has issued several resolutions pertaining to employees’ consent for certain data treatment.

e. Online/Electronic Consent
Electronic records are acceptable under Uruguayan Law. Notwithstanding, validity of the data subject’s consent will depend on compliance with the abovementioned requirements established by the law. It should be underlined that electronic consent would not be sufficient in case of treatment of sensitive data, in which case written consent is required.

6. Information/Notice Requirements
Under Uruguayan Data Protection Law, whenever personal data is collected and processed, regardless of the need to obtain prior consent, data subjects should be informed of the following:

- The purpose for which data shall be processed and who may be the recipients or categories of recipients of the data.
- The existence of the corresponding database, whether electronic or any other type, and the identity and address of the data controller.
Whether replies to the proposed questionnaire are mandatory or voluntary, particularly regarding sensitive data.

Consequences of the provision of data and of the refusal to do so, or their inaccuracy.

The data subject’s possibility of exercising his/her rights of access rectification and deletion his/her data.

7. Processing Rules

When processing personal data, both data controllers and data processors ought to comply with the principles of the law detailed in the previous sections.

Furthermore, the Law establishes that when third parties provide personal data processing services, said personal data may not be used for a purpose not specified in the service agreement, neither may the data be given to other persons, even for storage thereof. Once the contractual service has been provided, the processed personal data should be destroyed, except upon express authorization of the service provider in those situations in which there is a reasonable presumption that there may be further orders. If this is the case, the personal data may be stored with the appropriate security conditions for a period of up to two years.

8. Rights of Individuals

The Law grants data subjects certain rights regarding their personal data. These are the rights of access, rectification, inclusion and suppression (deletion) of their data, as well as the right to update their data.

The right of access implies that data subjects, whether natural persons or legal entities, having proved their identity with the corresponding identity card or respective proxy, shall have the right to obtain any information on themselves registered in any database. Said right shall only be exercised free of charge within six-month intervals, unless a legitimate interest arises prior to the lapse of the 6-month period according to the local legal framework. The exercise of the right of a deceased person concerning his/her personal data shall belong to any of his/her duly proven universal successors.

The information requested must be provided to the data subject in a clear way, which should not be encoded, in which case it shall be accompanied by an explanation of the terms used, in a language accessible to the average knowledge of the population. Moreover, the information shall be comprehensive and associated to the entire record belonging to the data subject, even when the request only includes one aspect of his/her personal data. In no case shall the report disclose data belonging to third parties, even when related to the interested person. The data subject may choose whether the information should be provided in writing or through electronic, telephone, imaging or similar appropriate media for such purpose.
As regards the remaining rights, persons or legal entities shall have the right to request the rectification, updating, inclusion or deletion of their personal data included in a database, when verifying an error, falseness or when requesting for exclusion of certain information.

The deletion or suppression of personal data shall only proceed in the following cases:

a. Damages to the rights and legitimate interests of third parties.

b. Obvious error

c. Contravention of a legal obligation.

During the process of verification, rectification or inclusion of personal data, the data controller, upon third parties’ request to access reports on such data, shall record the fact that said information is subject to review. In the case of data transfer or communication, the data controller must notify the rectification, inclusion or deletion to the recipient within five working days after the data processing is carried out.

The rectification, updating, inclusion, erasure or deletion of personal data, when appropriate, shall be carried out free of charge for the data subject.

Whenever data subjects exercise any of the rights detailed on this section, the data controller shall have five business days to either comply with the request to access, update, delete, rectify or include, or to state the reasons why it considers it not appropriate to do so. Once the aforementioned period has expired without any of the foregoing situations having taken place, the data subject shall have the right to initiate a “habeas data” action before a Court of Law.

9. Registration/Notification Requirements

The principle of legality provides that the formation of a database will be lawful when the database is properly registered. The Law establishes the obligation of data controllers to duly register all its databases before the local Data Protection Authority.

The Decree establishes the steps to be undertaken in order to file for the registration of databases, as well as the information required to be disclosed to the Data Protection Authority in connection to said filing.

10. Data Protection Officers

In Uruguay, there is no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.
11. International Data Transfers

It is prohibited to transfer any personal data to countries or international organizations that do not offer proper protection in accordance with the standards of International or Regional Law on this matter.

This prohibition does not apply in the cases of:

1. International judicial cooperation, in accordance with the corresponding international instrument, this being either a Treaty or a Convention, with the particular circumstances under consideration.

2. Exchange of medical information, whenever required for the treatment of patients either for health or public hygiene reasons.

3. Bank or stock exchange transactions, pertaining to the respective transactions and in accordance with the applicable legislation.

4. Agreements within the framework of international treaties agreed upon by the Oriental Republic of Uruguay.

5. International cooperation among intelligence organizations to fight against organized crime, terrorism and drugs trade.

International transfer of data may also be possible in the scenarios mentioned below:

A. The interested party has given his/her unmistakable consent to the intended transfer.

B. The transfer is required to execute a contract between the interested party and the data processor or to execute pre-contractual measures taken at the interested party’s request.

C. The transfer is required to enter into or execute a contract entered into, or to be entered into on behalf of the interested party, between the data processor and a third party.

D. The transfer is required or demanded by law to protect a major public interest, or to acknowledge, exercise or defend a right in a judicial procedure.

E. The transfer is required to protect the vital interest of the interested party.

F. The transfer takes place from a registry, which is created, by virtue of legal or regulatory provisions, to release information to the public and receive queries from the general public or from any person who may prove that he/she has a legitimate interest, as long as the conditions established by law for the query are met, for each particular case.
Without prejudice to the above, the local Data Protection Authority may authorize international transfers of personal data to a third country which does not guarantee the proper protection, if the data controller offers the necessary guarantees for the protection of private life, of essential rights and freedoms of people, as well as guarantees for the exercise of their respective rights. Said guarantees may stem from the corresponding contractual clauses.

As a final note, international transfers of data within multinational companies (i.e. affiliates, subsidiaries, branches, parent company) would be permitted if the local entity (data controller) files for the registration of a Code of Conduct (type of Corporate Binding Rules) before the local Data Protection Authority, which will govern such transfers.

The local Data Protection Authority has issued a Resolution stating that countries deemed as providing the required levels of personal data protection include the European Union, as well as those that the European Commission has granted the adequacy note.

12. Security Requirements

In order to comply with the Principle of Data Security, the data controller or user of the database must take the necessary steps to ensure the security and confidentiality of personal data. Such measures must include the prevention of the alteration, loss or unauthorized data treatment, as well as detection of any re-direction of information, intentional or not, whether the risks come from human action or from the technical means used.

The Law expressly prohibits the inclusion of personal data within databases that do not comply with the technical conditions of integrity and security.

The local Data Protection Authority has suggested that data controllers adopt the parameters established by ISO 27001 in order to comply with the obligations of the Law.

13. Special Rules for Outsourcing of Data Processing to Third Parties

The Law establishes that when third parties provide personal data processing services, said personal data may not be used for a purpose not specified in the service agreement; neither may the data be given to other persons, even for storage thereof. Once the contractual service has been provided, the processed personal data should be destroyed, except upon express authorization of the service provider in those situations in which there is a reasonable presumption that there may be further orders. If this is the case, the personal data may be stored with the appropriate security conditions for a period of up to two years.
14. Enforcement and Sanctions

The local Data Protection Authority is empowered to apply sanctions to data controllers or data processors whenever the provisions of the Law are infringed.

The sanctions are graduated according to the level of severity of non-compliance, the relapse of the non-compliant entity, and the damage, as follows:

1. Observation, when the infringement is very slight.
2. Warning, when the infringement is slight and the controller has no previous record of any other infringement.
3. Fine, when the infringement is slight and there is previous record of other infringement, or whenever the infringement is severe or very severe.
4. Suspension of the corresponding database when the infringement is very severe.
5. Closing of the corresponding database when the infringement is very severe.

The Suspension and Closing of databases are to be applied when the infringement is very severe and the fine is not sufficiently adequate to address the violations of the Privacy Act.

In practice, the local Data Protection Authority does not have a policy of active control, but it acts upon claims of the data subjects.

15. Data Security Breach

The Decree establishes that whenever an occurrence of a data security breach likely to affect the interests of data subjects in a significant manner comes to the knowledge of the data controller or data processor regardless of the phase of processing, the data subjects shall be informed of such situation.

16. Accountability

According to local regulation, the data controller is accountable to the data subjects and the local Data Protection Authority for non-compliance with the Law. Accordingly, the local Data Protection Authority may impose sanctions for violations of the Law. In addition, the data subjects may resort to habeas data actions when rights related to their personal data are compromised. Data subjects could further claim damages via a judicial procedure in case a breach of the law concerning the treatment of their personal data results in damage to them.
17. Whistle-blower Hotline

In Uruguay, while there is no specific law or regulation on whistle-blowing, a document referred to by the Spanish Regulator, issued by the WP117 concerning whistle-blowing in the field of accounting and internal auditing, which has been previously applied to other cases of whistle-blowing within the labor relationship context, may be used for reference. Said document establishes certain requirements to be fulfilled when a company installs a whistle-blowing program.

18. E-Discovery

There is no specific law or regulation in Uruguay on e-discovery.

Notwithstanding this, following the parameters of the Law, when implementing an e-discovery system, an organization may be required to: obtain the consent of employees if the collection of personal data is involved; and advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

There is no specific law or regulation in Uruguay on anti-spam filtering solutions.

Notwithstanding this, following the parameters of the Law, when implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.

20. Cookies

There is no specific regulation requiring the collection of data subjects’ consent before putting cookies or other tracking technologies on their devices. Nevertheless, consumers ought to be duly informed of the fact that said technologies will be activated, the manner to disable the same, and the consequences for deactivating them. In practice the most common manner to comply with the latter is through a clause within the site’s Privacy Policy.

21. Direct Marketing

The Law establishes that in the collection of addresses, the distribution of documents, advertising, commercial prospecting, sale or other similar activities, appropriate data may be processed to establish specific profiles with promotional, business or advertising purposes; or that help determine consumer habits, whenever they appear on publicly accessible documents or are provided by the data subjects themselves or obtained with their consent.

In the scenarios envisaged above, the data subject may exercise the right of access free of charge. And at any time, the data subject may request the removal or blocking of his/her data from the databases.
Accordingly, local regulation provides for:

- an opt-in option, except in those cases where the data is collected from public sources of information, and
- an opt-out possibility, which implies that the data subjects can request his/her removal from the database created for marketing/promotional purposes at any time, and that in every communication to the data subject, the option to be removed from the database shall be provided.
Venezuela

**Maria Eugenia Salazar**  
Caracas  
Tel: +58 212 276 5161  
mariaeugenia.salazar@bakermckenzie.com

**Luis Miguel Vicentini**  
Caracas  
Tel: +58 212 276 5069  
luis.miguel.vicentini@bakermckenzie.com
1. Electronic Commerce

Since May 2000, the Venezuelan Government decreed the access to and use of the Internet as a priority policy for the country’s cultural, economic, social and political development.

Fortunately, the Venezuelan legal framework is sufficiently broad and flexible, so it is not necessary to generate a large number of new “e-” regulations, but only to adjust the existing ones to this new mode of business. The following is a description of the main legal aspects that should be considered when entering into “online” contracts, maintaining B2B and B2C businesses, including the advertising activities and the handling of personal data and intellectual property within the context of the cyberspace.

• The Law on Data Messaging and Electronic Signatures

The Law on Data Messaging and Electronic Signatures (the “LMD”) was a major step for Venezuela to enter into the new digital economy, since in a timely fashion it settles the main deficiencies of our legal system regarding this interesting business medium. Particularly, the LMD facilitates and promotes electronic commerce through the use of data messages and electronic signatures that are legally valid and enforceable, thus restoring the reliability, which is a fundamental element for commerce that was seriously impaired by the lack of clear rules.

The purpose of this law is to (i) grant and acknowledge the legal effect and value of electronic signatures; (ii) grant and acknowledge the legal effect and value of data messages and all intelligible information in electronic format (regardless of its material support); (iii) regulate all matters pertaining to providers of certification services, and (iv) regulate all matters related to electronic certificates. The LMD is closely related to electronic commerce and online transactions, whereas it sets forth clear rules for the fundamental components of the exchange of goods and services through the Internet.

• The Electronic Signature

The LMD grants legal value to and acknowledges the effect of the “electronic” signature, not simply as a “digital” signature, deviating from a regulatory trend that is limited to acknowledging legal value only to the signatures made with asymmetric encryption technology (“digital” signatures), a technological sub-species of the electronic signature genre that includes, in addition to the digital signature, the symmetric encryption signature and any other information created or used by the signatory that is related to the data messages and enables ascribing authorship.
The will of the parties

The LMD contains supplement rules to the will of the parties regarding the establishment of the issuer’s identity, the time when the message is deemed to be issued and received, the place of issuance and receipt, acknowledgments of receipt, and an express reference to contractual matters that enables the parties to agree that the offer and the acceptance be made through data messages.

The Superintendence of Electronic Certification Services

Finally, the LMD creates the Superintendence of Electronic Certification Services (“SUSCERTE”), as a service with budgetary, administrative, financial and management autonomy, and has the purpose of accrediting, supervising and controlling the public or private Certification Services Providers (“CSP”) upon the terms set forth in the LMD and its regulations. In this regard, the SUSCERTE has currently certified at least two companies as CSP.

2. Data Privacy

a. Legal Framework

(i) Constitution

(ii) Law Protecting the Privacy of Communications

(iii) Law of Data Processing Crimes

(iv) Law of Data Messages and Electronic Signatures

(v) Supreme Court Decision of August 4, 2011 which develops Article 28 of the Constitution (The “August 4, 2011 SC Decision”)

(vi) Supreme Court Decision of March 14, 2001

b. Definition of Personal Data

Personal Data is defined as the combined information that could create a complete or partial profile of an individual (Supreme Court Decision of March 14, 2001)

c. Data Owner Rights

The Constitution provides:

(i) Protection of the secrecy of private communications;

(ii) Right to be informed of how entities are using personal data

(iii) Right to access registries with personal data

(iv) Right to file a court action (habeas data) to update, correct or destroy registries with inaccurate or prejudicial data

(v) Right to access documents of interest to communities or groups of people
The above mentioned rights were interpreted by the Supreme Court in the August 4, 2011 SC Decision in nine data privacy principles that are summarized as follows:

1. **Autonomy of Will**
   (a) Inform data owner about
   i. Collection of data
   ii. Entity responsible
   iii. Purpose
   iv. How self-determination can be exercised
   (b) Disclosure of data is subject to prior, free, informed, unequivocal and revocable consent

2. **Legality**
   (a) Information cannot be used for purposes contrary to the principles of the August 4, 2011 SC Decision
   (b) Cannot be processed by illegal or unfair methods

3. **Purpose and Quality**
   (a) Data must be compiled with a clear purpose, reason or cause - essential for validity of consent

4. **Temporality and Preservation**
   (a) Data must be updated regularly and it must be preserved accurately and completely, in a safe manner to avoid data lost.

5. **Accuracy and Self-Determination**
   (a) Data owner must have access to data
   (b) Data owner can demand correction or cancellation of incomplete, inaccurate, inadequate and excessive data and has the right to be notified of the correction

6. **Foresight and Integrality**
   (a) Take technological advances into account so as not to prejudice data owner’s rights or interests.

7. **Safety and Confidentiality**
   (a) Obligation to keep data secure and prevent third party modification -
   (b) This obligation survives the termination of the relationship
(c) Transfer of data to other states that don’t have the same guarantees is prohibited

8. Protection

(a) Judicial protection is not sufficient; public entities must establish framework

9. Responsibility

(a) Violation gives rise to civil, criminal and administrative penalties

d. Data Transfer

(i) The August 4, 2011 SC Decision set forth that data can only be transferred to jurisdictions which provide the same protection as the Venezuelan laws do.

(ii) It must be carefully noted that the transfer of personal data from Venezuela to countries which do not offer legal protection to personal data at the same level that Venezuelan regulations do, is not permitted.

The nine principles prescribed by the August 4, 2001 SC Decision commented above, have not yet been developed. However, the standards provided therein should be followed before transferring the data to a different jurisdiction. In any event, a detailed comparison and analysis of Venezuelan laws and the laws of the country where the data is going to be transferred, is strongly recommended.

The data owner’s prior, free, informed, unequivocal and revocable consent is required before the transferring of the data is performed.

e. Data Owner Consent

(i) Venezuela is an opt-in country. Data owner’s prior and express consent must be given for the collection of his/her personal data. To provide their consent, data owner should be able to have a special tool such as clicking a button or ticking an unchecked box.

f. Unlawful Conducts Related to Personal Data

1. Pursuant to the Law of Data Processing Crimes, the following conducts against the personal data and communications are unlawful:

(a) To obtain, modify or eliminate any information contained or concealed in data processing systems without the consent from its lawful owner.

(b) To access, capture, interfere, reproduce, modify, deviate or eliminate, by means of any data processing technology, any data message, transmission signal or any other communication of a third party.
(c) To publish any information obtained by unlawful methods as described in the law.

2. Pursuant to the Law Protecting the Privacy of Communications, the following conducts are unlawful:
   (a) To record any communication between any persons.
   (b) To install any recording equipment to illegally record or obstruct any communication.
   (c) To alter, damage or forge the content of any communication for the obtainment of personal benefit.
   (d) To cause emotional distress on other persons, by the utilization of unlawfully obtained information.
Vietnam

Andrew Fitanides  
Ho Chi Minh City  
Tel: +84 8 3520 2687  
andrew.fitanides@bakermckenzie.com

Tran Manh Hung  
Hanoi  
Tel: +84 4 3936 9398  
tmh@bmvn.com.vn

Minh Tri Quach  
Hanoi  
Tel: +84 4 3936 9605  
minhtri.quach@bmvn.com.vn

Yee Chung Seck  
Ho Chi Minh City  
Tel: +84 8 829 6234  
yeechung.seck@bakermckenzie.com
1. Recent Privacy Developments

2013 witnessed several important developments in Vietnam’s privacy-related law. Both Decree No. 72 and Decree No. 52 helped to clarify the definition of “personal information” that is afforded legal protection. Decree No. 72 also provides general provisions on data privacy, while Decree No. 52 addresses data privacy in the context of e-commerce. Finally, the Vietnamese authorities issued Decree No. 158, Decree No. 174 and Decree No. 185 stipulating the applicable sanctions for, among other things, violations of Vietnam’s privacy-related laws.

Both Decree No. 72 and Decree No. 52 define “personal information” protected under the law similarly to the European Union’s Data Protection Directive. Specifically, Decree No. 72 defines protected “personal information” as “information associated with the identification of individuals.” In the context of e-commerce, Decree No. 52 defines “personal information” as “information contributing to the identification of a specific individual, including his/her name, age, home address, phone number, medical information, account number, information on personal payment transactions and other information that the individual would like to keep confidential.”

Decree No. 52 and Decree No. 72 also create exceptions where “personal information” may be collected, used and transferred without prior consent if:

- pursuant to a decision of an authorized State Agency;
- the information has been publicized on e-commerce websites by the data subject;
- the information is used for:
  - signing, modifying or performing contracts for the use of information, products or services in a network environment;

---

1 Decree No. 72/2013/ND-CP dated 15 July 2013, on the management, provision, and use of internet services and online information (“Decree No. 72”).
2 Decree No. 52/2013/ND-CP dated 16 May 2013, on e-commerce (“Decree No. 52”).
3 Decree 158/2013/ND-CP dated 12 November 2013 on penalties for administrative violations pertaining to culture, sports, tourism and advertising (“Decree No. 158”).
4 Decree 174/2013/ND-CP dated 13 November 2013 providing penalties for administrative violations pertaining to postal, telecommunication, information technology and radio frequency areas (“Decree No. 174”).
5 Decree 185/2013/ND-CP dated 15 November 2013 providing penalties for administrative violations pertaining to trading activities, production, trade of counterfeiting or prohibited goods, and protection of consumer’s rights (“Decree No. 185”).
6 Directive 95/46/EC, of 24 October 1995, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.
Decree No. 72 also introduces general provisions that distinguish between "private information," defined as "the online information of an organization or individual that is not publicized by that organization or individual, or has only been provided for a group of receivers that are identified," and "public information," which is defined as "online information of an organization or individual that is publically provided without identifications or addresses of its receivers." These definitions appear to distinguish between the duties that data custodians owe to Data Subjects based on the type of data in their possession. However, the foregoing definitions also suggest that certain private information belonging to organizational Data Subjects may be protected and also represent a first step towards the creation of the "Sensitive" Data a category as seen in other jurisdictions.

Decrees No. 158, No. 174 and No. 185 provide the following penalties for violations of Vietnam's privacy-related laws:

- a fine of between VND30 million to VND40 million for disclosing or transferring personal information of customers in an e-commerce transaction without prior consent.7
- a fine of between VND10 million to VND20 million for failing to put in place measures to protect the personal information of data subjects, or for the collection, processing or use of a data subject’s personal information without his or her prior consent.8
- a fine of up to VND15 million for the act of sending an advertising message or email without a recipient’s prior consent.9

2. Emerging Privacy Issues and Trends

The Government of Vietnam continues its efforts to regulate on-line activities in order to, among other things, exert greater control over content published on the Internet. New regulations in this area will likely affect the privacy rights of individuals subject to Vietnamese law.

The Draft Law on Information Security indicates that the Government of Vietnam may require companies “engaged in activities on networks” to take an active role in preventing and removing prohibited content from their networks - thus impacting the privacy rights of network users.

---

7 Article 82.4(b) of Decree No. 185.
8 Articles 66.3(d) and (e) of Decree No. 174.
9 Article 56.1(b) of Decree No. 158.
The Draft Law on Information Security also requires that data custodians remove personal information stored in their databases after the purpose for which the information was collected no longer exists, or after the announced storage period has expired. These provisions may indicate that Vietnam’s privacy-related law is moving towards a European data-privacy model, albeit without limitations on the Vietnamese government’s own collection, use and transfer of “personal information.”

As discussed in Section 1 above, Decree No. 72 introduces the concept of organizational “private information” that is entitled to protection under Vietnamese law. New regulations covering the responsibilities of data custodians may build upon the concept of “private information” to elaborate on the privacy rights applicable to organizations under Vietnamese law.

3. Applicable Law

- Law No. 33/2005/QH12, adopted by the National Assembly on 14 June 2005, ("Civil Code"); Part 1 Chapter 3, Section 2 addresses the personal rights of individuals. Article 31 pertains to the rights of an individual with respect to his or her image. Article 38 pertains to the right of an individual to maintain the confidentiality of certain personal information;

- Law No. 67/2006/QH11, adopted by the National Assembly on 29 June 2006 ("IT Law");

- Law No. 51/2005/QH11, adopted by the National Assembly on 29 November 2005 ("E-Transactions Law");

- Law No. 59/2010/QH12, adopted by the National Assembly on 17 November 2010 ("Consumer Protection Law");


- Decree No. 99/2011/ND-CP guiding the implementation of the Consumer Protection law, issued by the Government on 27 October 2011 ("Decree No. 99");

- Decree No. 72/2013/ND-CP dated 15 July 2013, on the management, provision, and use of internet services and online information ("Decree No. 72");

- Decree No. 64/2007/ND-CP, dated 10 April 2007, of the Government on application of information technology in State agency activities ("Decree No. 64");

- Decree No. 90/2008/ND-CP on Anti-Spam, dated 13 August 2008 ("Decree No. 90");
4. Key Privacy Concepts

a. Personal Data

Vietnam does not have a single comprehensive law that addresses individual and organizational privacy rights. Instead, relevant provisions are contained in the Civil Code, the IT Law, the Consumer Protection Law, the Penal Code, the Telecommunications Law and the specialized regulations (where applicable), though these matters are addressed in fairly general terms, and in related implementing regulations that contain more specific provisions.

As a general principle, these laws protect information pertaining or belonging to individuals or (to a lesser degree) organizations that is personal or private in nature (“Protected Information”).

However, the Civil Code, the Penal Code, the IT Law, the Consumer Protection Law and the Telecommunications Law do not clearly define what information constitutes Protected Information. The Civil Code refers to “information and materials on the private life of an individual,” while the Penal Code merely identifies the media by which the transmission of Protected Information is protected. Similarly, the IT law uses the term “personal
“personal information” without providing a definition of what this entails. The Telecommunications Law defines “personal information” in the context of call log data that telecommunication providers must protect and keep secure.

Decree No. 72, which was issued in 2013, regarding online content, defines personal information as “information associated with the identifications of individuals, including names, ages, addresses, ID numbers, phone numbers, email addresses, and other information defined by law.” Decree No. 72 also introduces the concept of “private information,” which it defines as “the online information of an organization or individual not publicized by that organization or individual, or only provided for a group of receivers that are identified.” Article 3.14 of Decree No. 72 also defines “public information” as “online information of an organization or individual publically provided without identifications or addresses of receivers.”

In the context of e-transactions, Decree No. 52 defines “personal information” as “information contributing to identify a specific individual, including his/her name, age, home address, phone number, medical information, account number, information on personal payment transactions and other information that the individual would like to keep confidential.”

b. Data Processing

Article 21 of the IT Law requires organizations or individuals that collect, process, and use the personal information of other persons in the network environment obtain the data subject’s consent. They must also notify the Data Subject of the form, scope, place and purpose of the processing of his or her personal information. Organizations and individuals are entitled to collect, process, and use the personal information of an individual without his or her consent where the personal information is used for the following purposes:

- the signing, modifying or performing of contracts for the collection, processing and use of information, products or services in the network environment;
- pricing or calculating charges for the use of information, products or services in the networked environment; and
- performing other obligations in accordance with the law.

c. Processing by Data Controllers

Control of mail, telephone, electronic mail, and other forms of electronic information may be conducted only in cases where the law permits and pursuant to an authorized State body’s decision.

Under Article 22 of the IT Law, organizations or individuals that store personal information in the network environment must not transfer said information to any third party without the data subject’s consent, unless otherwise provided by law.
d. Jurisdiction/Territory
There is no provision that specifically limits the scope of privacy laws to the jurisdiction/territory of Vietnam.

e. Sensitive Personal Data
Although the concept of Sensitive Personal Data does exist in Vietnamese law, it is not well-developed concept. Decree No. 72 defines “private information” as “the online information of an organization or individual not publicized by that organization or individual, or only provided for a group of receivers that are identified.” Decree No. 72 prohibits any illegal use of private information and requires that the state authorities’ control of online private information must be conducted in accordance with the law. Decree No. 72 also requires social network services providers take measures to protect users’ private information.

In addition, regulations also protect certain data, such as medical records, against illegal disclosure and use.

f. Employee Personal Data
The New Labor Code contains some specific information on employee data.

5. Consent

a. General
Consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data, subject to certain prescribed exceptions. (See Section 1)

Consent is contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

In general, consent may be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to cover only the identified purpose(s). There is no mandatory requirement for consent to be in writing. Consent may be provided orally or in different forms and formats. In addition, the Data Subject also has the right to withdraw consent at any time.

Consent does not need to be in the local language, provided that the Data Subject understands the language in which consent is given.

b. Sensitive Data
The concept of Sensitive Data is not well-developed in Vietnam. Generally, the collection and publication of information and data about the private life of an individual requires that person’s consent.
c. **Minors**
For a person under the age of 15, Vietnamese law requires the consent of a parent or other representative before information or data concerning the minor’s private life may be collected.

d. **Employee Consent**
The New Labor Code contains specific information on employee data. In general, employee consent is required to collect and process an employee’s Personal Data.

e. **Online/Electronic Consent**
In Vietnam, online or electronic consent is permissible and is deemed effective if properly structured and evidenced.

6. **Notice Requirements**
An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity, the types of Personal Data being collected; the purposes for collecting Personal Data; third parties to which the organization will disclose the Personal Data; the rights of the Data Subject; how the Personal Data is retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; and how to access and/or correct the Data Subject’s Personal Data.

7. **Processing Rules**
An organization that processes Personal Data must limit the use of Personal Data to only those activities that are necessary to fulfill the identified purpose(s) for which the Personal Data was collected.

8. **Rights of Individuals**
Data Subjects have the general right to: be informed by the organization that holds the Data Subject’s Personal Data and how the Data Subject’s Personal Data is being processed; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. **Registration/Notification Requirements**
There is no authority tasked specifically with administering the collection, process, use and transfer of personal data in Vietnam. However, an organization that collects and processes certain types of Personal Data may be required to follow procedures that may include registration or notification with the relevant authority.
10. Data Protection Officers
In Vietnam, there is no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers
Although there is no provision that specifically addresses international data transfers, organizations or individuals may not supply the personal information of an individual without obtaining the consent of that person or unless otherwise provided by law.

12. Security Requirements
Organizations are required to protect Personal Data in its possession and control from unauthorized access and use. These organizations must implement appropriate physical, technical and organization security safeguards to protect said Personal Data.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties may be required to use contractual or other means to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors. In case a data breach occurs, the outsourcing organization may be held liable together with the third party provider.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, and/or criminal proceedings.

15. Data Security Breach
Circular No. 27 defines a data security breach as a type of “Internet incident.” Circular No. 27 also creates an Internet incident response network to coordinate responses to all harmful Internet incidents, including those that involve data security breaches. Under Circular No. 27, organizations and individuals must report Internet incidents that they are unable to handle on their own to one or more of the following members of the incident response network: the network member responsible for incident response for that user (if any), the ISP that directly supplies Internet services to the user, and/or the Vietnam Computer Emergency Response Team (“VNCERT”).

For serious Internet incidents, Circular No. 27 requires immediate reporting to VNCERT. Serious incidents include those that occur on a large scale, spread
quickly, threaten serious harm to computer and Internet network systems, cause serious loss of information or which require substantial national or international resources to resolve. An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions and/or class actions.

16. Accountability
Currently, Vietnam does not have any laws that require organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. It is also not a requirement to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

17. Whistle-blower hotline
Whistle-blower hotlines may be established in Vietnam if they comply with local laws.

18. E-discovery
When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of personal data is involved. Related to the foregoing, the organization must advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization may be required to inform employees of the monitoring policies being implemented in the workplace, particularly if the collection of personal data is involved. The organization must afford the employees with an opportunity to review the isolated emails designated as spam.

20. Cookies
There are no specific laws/rules that regulate the use of cookies. Nonetheless, the use of cookies would have to comply with data privacy laws.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which the organization cannot inferred from a Data Subject’s failure to respond. Opt-out consent is permissible.
Baker & McKenzie Offices Worldwide

Office phone numbers and addresses change from time to time. Please refer to [www.bakermckenzie.com](http://www.bakermckenzie.com) for current contact information.

**Argentina - Buenos Aires**
Baker & McKenzie SC
Avenida Leandro N. Alem 1110, Piso 13
C1001AAT Buenos Aires
Argentina
Tel: +54 11 4310 2200
Fax: +54 11 4310 2299

**Australia - Brisbane**
Baker & McKenzie
Level 8
175 Eagle Street
Brisbane QLD 4000
Australia
Tel: +61 7 3069 6200
Fax: +61 7 3069 6201

**Australia - Melbourne**
Baker & McKenzie
Level 19
181 William Street
Melbourne VIC 3000
Australia
Tel: +61 3 9617 4200
Fax: +61 3 9614 2103

**Australia - Sydney**
Baker & McKenzie
Level 27, A.M.P. Centre
50 Bridge Street
Sydney, NSW 2000
Australia
Tel: +61 2 9225 0200
Fax: +61 2 9225 1595
Austria - Vienna
Diwok Hermann Petsche
Rechtsanwälte GmbH
Schottenring 25
1010 Vienna
Austria
Tel: +43 1 24 250
Fax: +43 1 24 250 600

Azerbaijan - Baku
Baker & McKenzie - CIS, Limited
The Landmark Building
96A Nizami Street
Baku AZ1010
Azerbaijan
Tel: +994 12 497 18 01
Fax: +994 12 497 18 05

Bahrain - Manama
Baker & McKenzie Limited
18th Floor, West Tower
Bahrain Financial Harbour
PO Box 11981, Manama
Kingdom of Bahrain
Tel: +973 1710 2000
Fax: +973 1710 2020

Belgium - Antwerp
Baker & McKenzie CVBA/SCRL
Meir 24
2000 Antwerp
Belgium
Tel: +32 3 213 40 40
Fax: +32 3 213 40 45

Belgium - Brussels
Baker & McKenzie CVBA/SCRL
Louizalaan 149 Avenue Louise
Eleventh Floor
Brussels 1050
Belgium
Tel: +32 2 639 36 11
Fax: +32 2 639 36 99

Belgium - ELC
Baker & McKenzie CVBA/SCRL
149 Avenue Louise
Eighth Floor
1050 Brussels
Belgium
Tel: +32 2 639 36 11
Fax: +32 2 639 36 99

Brazil - Brasilia
Trench, Rossi e Watanabe Advogados
SAF/S Quadra 02, Lote 04, Sala 203
Edificio Comercial Via Esplanada Brasilia - DF - 70070-600
Brazil
Tel: +55 61 2102 5000
Fax: +55 61 3327 3274

Brazil - Porto Alegre
Trench, Rossi e Watanabe Advogados
Av. Borges de Medeiros, 2233 - 4th floor
90110-150
Porto Alegre - RS
Brazil
Tel: +55 51 3220 0900
Fax: +55 51 3220 0901

Brazil - Rio de Janeiro
Trench, Rossi e Watanabe Advogados
Av. Rio Branco, 1
19th floor Sector B
Ed. RB1 - 20090-003
Rio de Janeiro - RJ
Brazil
Tel: +55 21 2206 4900
Fax: +55 21 2206 4949
### Indonesia - Jakarta
Hadiputranto, Hadinoto & Partners
The Indonesia Stock Exchange
Building
Tower II, 21st Floor
Sudirman Central Business District
Jl. Jendral Sudirman Kav. 52-53
Jakarta 12190
Indonesia
Tel: +62 21 2960 8888
Fax: +62 21 2960 8999

### Kazakhstan - Almaty
Baker & McKenzie - CIS, Limited
Samal Towers, 8th Floor
97 Zholdasbekov Street
Almaty Samal-2, 050051
Kazakhstan
Tel: +7 727 330 05 00
Fax: +7 727 258 40 00

### Italy - Milan
Studio Professionale Associato a Baker & McKenzie
Piazza Meda, 3
Milan 20121
Italy
Tel: +39 02 76231 1
Fax: +39 02 7623 1620

### Italy - Rome
Studio Professionale Associato a Baker & McKenzie
Viale di Villa Massimo, 57
Rome 00161
Italy
Tel: +39 06 44 06 31
Fax: +39 06 4406 3306

### Luxembourg
Baker & McKenzie
10 - 12 Boulevard Roosevelt
2450 Luxembourg
Tel.: +352 26 18 44 1
Fax: + 352 26 18 44 99

### Malaysia - Kuala Lumpur
Wong & Partners
Level 21, The Gardens South Tower
Mid Valley City
Kuala Lumpur 59200
Malaysia
Tel: +603 2298 7888
Fax: +603 2282 2669

### Mexico - Guadalajara
Baker & McKenzie Abogados, S.C.
Blvd. Puerta de Hierro 5090
Fracc. Puerta de Hierro
Zapopan, Jalisco 45110
México
Tel: +52 33 3848 5300
Fax: +52 33 3848 5399

### Mexico - Juarez
Baker & McKenzie Abogados, S.C.
P.O. Box 9338 El Paso, TX 79995
P.T. de la República 3304, Piso 1
Juarez, Chihuahua 32330
México
Tel: +52 656 629 1300
Fax: +52 656 629 1399
**Mexico - Mexico City**
Baker & McKenzie Abogados, S.C.
Edificio Virreyes, Pedregal 24,
Piso 12
Lomas Virreyes / Col. Molino del Rey
México, D.F. 11040
México
Tel: +52 55 5279 2900
Fax: +52 55 5279 2999

**Mexico - Monterrey**
Baker & McKenzie Abogados, S.C.
Oﬁcinas en el Parque
Torre Baker & McKenzie Piso 10
Blvd. Antonio L. Rodríguez 1884 Pte.
Monterrey, N.L. 64650
Mexico
Tel: +52 81 8399 1300
Fax: +52 81 8399 1399

**Mexico - Tijuana**
Baker & McKenzie Abogados, S.C.
P.O. Box 1205 Chula Vista, CA 91912
Blvd. Agua Caliente 10611, Piso 1
Tijuana, B.C. 22420
México
Tel: +52 664 633 4300
Fax: +52 664 633 4399

**Morocco - Casablanca**
Baker & McKenzie Maroc
Ghandi Mall - Immeuble 9
Boulevard Ghandi
20380 Casablanca
Morocco
Tel: +212 522 77 95 95
Fax: +212 522 77 95 96

**Myanmar - Yangon**
Baker & McKenzie Yangon
1203 12th Floor Sakura Tower
339 Bogyoke Aung San Road
Kyauktada Township
Yangon
Myanmar
Tel: +95 1 255 056
Fax: +95 1 255 057

**The Netherlands - Amsterdam**
Baker & McKenzie Amsterdam N.V.
Claude Debussylaan 54
1082 MD Amsterdam
P.O. Box 2720
1000 CS Amsterdam
The Netherlands
Tel: +31 20 551 7555
Fax: +31 20 626 7949

**Peru - Lima**
Estudio Echecopar
Av. De la Floresta 497
Piso 5 San Borja
Lima 41
Peru
Tel: +51 1 618 8500
Fax: +51 1 372 7171/372 7374

**Philippines - Manila**
Quisumbing Torres
12th Floor, Net One Center
26th Street Corner 3rd Avenue
Crescent Park West
Bonifacio Global City
Taguig City 1634
Philippines
Tel: +63 2 819 4700
Fax: +63 2 816 0080
Poland - Warsaw
Baker & McKenzie Gruszczynski i Wspolnicy Attorneys at Law LP
Rondo ONZ 1
Warsaw 00-124
Poland
Tel: +48 22 445 3100
Fax: +48 22 445 3200

Qatar - Doha
Baker & McKenzie LLP
Al Fardan Office Tower
8th Floor
Al Funduq 61
Doha, PO Box 31316
Qatar
Tel: +974 4410 1817
Fax: +974 4410 1500

Russia - Moscow
Baker & McKenzie - CIS, Limited
White Gardens
9 Lesnaya Street
Moscow 125047
Russia
Tel: +7 495 787 2700
Fax: +7 495 787 2701

Russia - St. Petersburg
Baker & McKenzie - CIS, Limited
BolloevCenter, 2nd Floor
4A Grivtsova Lane
St. Petersburg 190000
Russia
Tel: +7 812 303 9000
Fax: +7 812 325 6013

Saudi Arabia - Jeddah
Legal Advisors in Association with
Baker & McKenzie Limited
Bin Sulaiman Center, 6th Floor,
Office No. 606
Prince Sultan Street and
Rawdah Street Intersection
Al-Khalidiyah District
P.O. Box 128224
Jeddah 21362
Saudi Arabia
Tel: + 966 12 606 6200
Fax: +966 12 692 8001

Saudi Arabia - Riyadh
Legal Advisors in Association with
Baker & McKenzie Limited
Olayan Complex
Tower II, 3rd Floor
Al Ahsa Street, Malaz
P.O. Box 4288
Riyadh 11491
Saudi Arabia
Tel: +966 11 265 8900
Fax: +966 11 265 8999

Singapore
Baker & McKenzie. Wong & Leow
8 Marina Boulevard
#05-01 Marina Bay Financial Centre
Tower 1
Singapore 018981
Tel: +65 6338 1888
Fax: +65 6337 5100

South Africa – Johannesburg
Baker & McKenzie Johannesburg
4 Sandown Valley Crescent,
Sandton, 2196
Johannesburg
South Africa
Tel: +27 11 911 4300
Fax: +27 11 784 2855
<table>
<thead>
<tr>
<th>Country</th>
<th>City</th>
<th>Address</th>
<th>Tel</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>South Korea</td>
<td>Seoul</td>
<td>Foreign Legal Consultant Office</td>
<td>+82 2 6137 6800</td>
<td>+82 2 6137 9433</td>
</tr>
<tr>
<td>Spain</td>
<td>Barcelona</td>
<td>Baker &amp; McKenzie Barcelona S.L.P.</td>
<td>+34 93 206 0820</td>
<td>+34 93 205 4959</td>
</tr>
<tr>
<td>Spain</td>
<td>Madrid</td>
<td>Baker &amp; McKenzie Madrid S.L.P.</td>
<td>+46 8 566 177 00</td>
<td>+46 8 566 177 99</td>
</tr>
<tr>
<td>Turkey</td>
<td>Istanbul</td>
<td>Baker &amp; McKenzie Consultancy</td>
<td>+90 212 339 8100</td>
<td>+90 212 339 8181</td>
</tr>
<tr>
<td>Ukraine</td>
<td>Kyiv</td>
<td>Baker &amp; McKenzie - CIS, Limited</td>
<td>+380 44 590 0101</td>
<td>+380 44 590 0110</td>
</tr>
</tbody>
</table>
United States - San Francisco
Baker & McKenzie LLP
Two Embarcadero Center, 11th Floor
San Francisco, California 94111
United States
Tel: +1 415 576 3000
Fax: +1 415 576 3099

United States - Washington, DC
Baker & McKenzie LLP
815 Connecticut Avenue, N.W.
Washington, District of Columbia 20006
United States
Tel: +1 202 452 7000
Fax: +1 202 452 7074

Venezuela - Caracas
Baker & McKenzie SC
(Despacho de Abogados)
Centro Bancaribe, Intersección
Avenida Principal de Las Mercedes con inicio de Calle Paris,
Urbanización Las Mercedes Caracas 1060
Venezuela
Tel: +58 212 276 5111
Fax: +58 212 993 0818; 993 9049

Venezuela - Valencia
Baker & McKenzie SC
Urbanización La Alegria
Postal Address: P.O. Box 1155
Valencia Estado Carabobo
Venezuela
Tel: +58 241 824 8711
Fax: +58 241 824 6166

Vietnam - Hanoi
Baker & McKenzie (Vietnam) Ltd.
(Hanoi Branch Office)
Unit 1001, 10th floor,
Indochina Plaza Hanoi
241 Xuan Thuy Street,
Cau Giay District
Hanoi 10000
Vietnam
Tel: +84 4 3825 1428
Fax: +84 4 3825 1432

Vietnam - Ho Chi Minh City
Baker & McKenzie (Vietnam) Ltd.
(HCMC)
12th Floor, Saigon Tower
29 Le Duan Blvd.
District 1
Ho Chi Minh City
Vietnam
Tel: +84 8 3829 5585
Fax: +84 8 3829 5618
Baker & McKenzie has been global since inception. Being global is part of our DNA.

Our difference is the way we think, work and behave – we combine an instinctively global perspective with a genuinely multicultural approach, enabled by collaborative relationships and yielding practical, innovative advice. Serving our clients with more than 4,200 lawyers in over 45 countries, we have a deep understanding of the culture of business the world over and are able to bring the talent and experience needed to navigate complexity across practices and borders with ease.