PREPARING FOR THE GENERAL DATA PROTECTION REGULATION

Digest
Preparing for the General Data Protection Regulation – Digest

December 2016

READERSHIP
CISOs, senior business representatives, information security professionals, legal, IT, and others with an interest in the General Data Protection Regulation.

PUBLISHED BY
Information Security Forum Limited
+44 (0)203 875 6868
info@securityforum.org
www.securityforum.org

PROJECT TEAM
Alex Jordan – Lead
Mark Sowerby – Contributor

REVIEW AND QUALITY ASSURANCE
Toby Stevens

DESIGN
Kim Whyte
Shane Kearney

WARNING
This document is confidential and is intended for the attention of and use by either organisations that are Members of the Information Security Forum (ISF) or by persons who have purchased it from the ISF direct. If you are not a Member of the ISF or have received this document in error, please destroy it or contact the ISF on info@securityforum.org. Any storage or use of this document by organisations which are not Members of the ISF or who have not validly acquired the report directly from the ISF is not permitted and strictly prohibited. This document has been produced with care and to the best of our ability. However, both the Information Security Forum and the Information Security Forum Limited accept no responsibility for any problems or incidents arising from its use.

CLASSIFICATION
Restricted to ISF Members, ISF Service Providers and non-Members who have acquired the report from the ISF.
Preparing for the General Data Protection Regulation

The European Union’s General Data Protection Regulation (GDPR) is the biggest shake-up of global privacy law for over 20 years. Adopted in April 2016, with enforcement due from 25 May 2018, the GDPR represents the culmination of over five years of effort to modernise data protection.

The EU Directive on Data Protection (95/46/EC) (the EU Directive), adopted in 1995, could not have anticipated the increasing importance and reach of the Internet, or the exponential growth in methods for the mass-processing of data, such as online retailing, search engines and social networks. In response to these needs, the GDPR has superseded the previous EU Directive to create a unifying data protection law for all EU Member States.

The GDPR applies to personal data relating to EU residents regardless of where it is processed. It redefines the scope of EU data protection legislation, forcing organisations worldwide to comply with its requirements. The ISF estimates that over 98% of Member organisations will be impacted as a result. While the GDPR is based on the same data protection principles as its predecessor, it introduces new rights for data subjects (identified or identifiable individuals) such as the rights to the erasure or restriction of the use of their personal data. It also places new demands on an organisation, for example designating a data protection officer and formally assessing data protection impacts. The GDPR enables supervisory authorities to impose tough penalties including potential fines of up to 4% of group turnover, or €20m.

Robust data protection is not simply a burden on an organisation; good data protection practices should protect both brand and reputation, and improve data quality. An organisation with mature data protection practices should be able to meet many of the GDPR’s requirements. The ISF Approach, shown in Figure 1, will help an organisation to prepare for the GDPR’s requirements. It recommends that an organisation should:

‒ determine the applicability of the GDPR to data processing activities
‒ evaluate the effectiveness of data protection controls
‒ assess the scope of data protection capabilities
‒ understand the consequences if the GDPR’s requirements are not met
‒ aim to comply by 25 May 2018.

An organisation may already understand the extent to which they are aiming to comply with the GDPR, and the risks associated with their approach. Those yet to determine their approach must start preparing immediately or accept substantial risks.

“The regulation will... create clarity for businesses by establishing a single law across the EU. The new law creates confidence, legal certainty and fairer competition.”
- Jan Philipp Albrecht MEP

Figure 1: The ISF Approach

This Digest builds on the ISF Briefing Paper, EU Data Protection Regulation: Compliance Goes Global. It summarises the key requirements of the new legislation and provides questions that an organisation can ask to understand how the GDPR will affect them. The contents of the Digest will be refined and validated with Members over the coming months to create an Implementation Guide for publication in the second quarter of 2017.
Putting data protection into context

Data protection is the combination of processes and technologies that ensure personal data is processed in accordance with an individual’s wishes and the requirements of the law. The GDPR is intended to uphold data subjects’ rights and provide a common legal mechanism for an organisation to process and share personal data.

**WHAT IS PERSONAL DATA?**

Personal data is any data relating to a data subject and can include information obtained directly from the data subject, from other sources, or inferred through processing or aggregation with other information. Where the data subject’s name and other details are absent, this data may still be personal in nature, depending on other information to which the organisation has access. If the organisation also has access to a data source that can be used to infer the identity of the data subject, such as a database linking record numbers to data subjects’ names, then the data will be considered to be personal. Personal data can include computerised data and paper records held in a filing system, and employee data is considered to be personal data.

**FEDERAL VERSUS SECTORAL DATA PROTECTION LEGISLATION**

The European Union and countries such as Australia, New Zealand, Canada and Russia, have ‘federal’ data protection laws that provide comprehensive protection of personal data regardless of industry, territory or usage. Other countries, most notably the United States and China, have adopted a ‘sectoral’ approach that applies different laws to individual industries, territories or uses of personal data. These differing approaches introduce complexity when transferring personal data between the different systems and when ensuring that the data is adequately protected.

**TRANSFERS OF PERSONAL DATA TO OTHER COUNTRIES**

European data protection laws mandate that personal data may not be transferred to jurisdictions that do not have equivalent data protection laws, unless suitable legal safeguards are in place. These safeguards can include treaties (e.g. the EU-US ‘Privacy Shield’), contractual protections to bind the recipient to the laws of the source country (‘model clauses,’ ‘binding corporate rules’) or obtaining unequivocal consent to the transfer from the individual.

**THE ROLE OF SUPERVISORY AUTHORITIES**

Most countries (including all European Union nations) have established supervisory authorities to oversee the use of personal data. These supervisory authorities (e.g. the Netherlands’ Autoriteit Persoonsgegevens, France’s CNIL or the UK’s Information Commissioner) are government-appointed bodies that have powers to inspect, enforce and penalise processing of personal data. In the US, a number of authorities enforce data protection requirements under the sectoral approach, most notably the Federal Trade Commission (FTC), which has substantial regulatory powers.

**DATA PROTECTION PRINCIPLES**

Data protection laws worldwide are generally built around foundational principles that determine how personal data should be processed. These principles dictate that data must be:

- processed lawfully, fairly and in a transparent manner
- collected only for specific, explicit and legitimate purposes, and not processed in a manner incompatible with the stated purposes
- adequate, relevant and limited to what is necessary
- accurate, and where necessary, kept up to date
- kept for no longer than is necessary
- processed in a secure manner.

An organisation must be able to demonstrate compliance with these principles.

**INFORMATION RIGHTS**

Data protection laws uphold data subjects’ rights when personal data relating to them is processed. The definitions in the GDPR include data subjects’ rights to:

- concise, transparent and easily accessible information, in clear and plain language, about the identity and contact details of the organisation, the purposes of processing, and any onward use of data
- access personal data or obtain copies in a machine-readable form
- rectify (amend) or erase personal data
- restrict the purposes of processing
- object to processing, automated decision-making or profiling.
The EU General Data Protection Regulation (GDPR)

The GDPR\(^1\) aims to strengthen EU residents’ fundamental rights and freedoms in the digital age and to provide enhanced protections for EU residents’ personal data. It also modernises and unifies diverse existing legislation across the EU Single Market, thus bringing greater legal certainty and reduced operating risk for companies that have to account for the diverse laws and enforcement regimes of 28 EU Member States when operating in Europe.

*The GDPR is an extensive legislative document, comprising almost 200 pages of legal arguments and requirements. It is broken down into two main sections, the introductory recitals and the 11 Chapters of the legislation itself. The 11 Chapters are broken down into 99 Articles, each of which deals with a different element of data protection law.*

The GDPR enforces new rights for EU residents and for any other data subjects whose data is processed in the EU, as well as placing new obligations on organisations and introducing new powers for supervisory authorities. A number of requirements, shown on the right, are particularly significant for an organisation and are summarised in this Digest.

**DEFINITIONS AND CASE LAW**

Like many new laws, the GDPR includes terms which have yet to be clearly defined. For example, the GDPR omits definitions of ‘large-scale’ processing, ‘without undue delay’ and ‘systematic monitoring’. Before the GDPR is enforced, supervisory authorities are likely to provide some guidance on these uncertain terms, but in practice, many will only become clear when they have been contested in a court of law.

**THE GDPR AND OTHER DATA PROTECTION REQUIREMENTS**

The GDPR is not the only data protection obligation with which an organisation needs to comply and therefore should be treated as part of a broader data protection management system that encompasses the people, processes and technologies used to control personal data processing. This can include requirements from a variety of sources, such as: local legislation, case law and treaties; sector-specific regulatory requirements; and commercial obligations arising from contractual terms and publicised organisational commitments for personal data processing (e.g. privacy notices and terms and conditions).

These sources, combined with an organisation’s values, attitude to risk and compliance demands, largely determine how personal data is protected. Whilst values, risk and compliance are often in tension, an organisation can take a holistic approach where its values guide the balance between risk and compliance.

---

Introducing the ISF Approach

The GDPR mandates an organisation to implement specified data protection controls and establishes personal data management capabilities by the enforcement deadline, or risk substantial penalties. The ISF Approach helps to interpret the key GDPR requirements and categorises GDPR requirements as either:

- **Controls**: where the GDPR mandates certain technical, procedural or personnel controls in an organisation that meets a minimum threshold, irrespective of risk levels or other considerations; or
- **Capabilities**: where the GDPR requires a particular outcome without describing specific people, process or technology controls to achieve the outcome, but instead describes a general capability, e.g. to be able to identify and erase all personal data relating to a specific data subject.

This approach provides a process to assess and manage data protection requirements in an organisation, and includes the following steps:

- **Determine applicability**: The organisation should examine its personal data processing activities to determine whether the GDPR applies and if so, identify the data, functions or business units (including third parties) who may process personal data on the organisation’s behalf, or with whom the organisation shares personal data.

- **Evaluate controls**: The GDPR requires an organisation to implement specific, defined controls over personal data if the number of records exceeds a certain size, a certain level of sensitivity, or when processing of personal data is the main activity of the organisation.

- **Assess capabilities**: The GDPR prescribes certain outcomes without defining how to achieve them and an organisation should understand whether it has the capabilities to achieve those outcomes.

- **Understand consequences**: Failure to uphold information rights can carry a fine of up to 4% of the organisation’s group turnover or €20m, whichever is the greater. Furthermore, failure to implement the specified controls can carry a fine of up to 2% of the organisation’s group turnover or €10m, even if information rights have been upheld. Just as significant is the potential impact of an enforcement that requires an organisation to suspend business activities whilst it remedies data protection problems, or the associated adverse publicity arising from a data protection incident. An organisation should ensure that these new consequences are reflected in risk assessments and mitigated by training, procedural, technical and legal controls.

- **Prepare for compliance**: The GDPR will be enforced from 25 May 2018 and an organisation should understand which aspects of its preparations will – or will not – be in place by that time so that they can plan their implementations and mitigate residual risks if they are not ready.
DETERMINE APPLICABILITY

The GDPR is now the primary data protection legislation in the European Union. It supersedes the previous EU Directive on Data Protection and EU Member States will need to repeal the elements of their national data protection laws that were derived from the Directive. As a European Regulation, it overrides EU Member State law should there be a conflict of laws. However, there are provisions (known as ‘derogations’) in the GDPR that allow EU Member States to modify some of the smaller elements of the Regulation, as well as to implement additional requirements that go above and beyond those of the GDPR. An organisation that is subject to other requirements, such as PCI-DSS, should seek to comply with both sets of requirements and where there is overlap or conflict, reach the higher standard of the two.

The GDPR extends beyond EU borders and its jurisdiction includes EU residents’ data no matter where in the world it is processed. European supervisory authorities can enforce the GDPR against an organisation even if it has no physical presence in the EU; so long as an organisation is processing EU residents’ data or monitoring their activities (e.g. profiling visitors to a website), the GDPR applies. The GDPR requires that any organisation outside of the EU that has obligations under the GDPR designates a representative within the EU to become an intermediary for the purposes of contact and enforcement actions. The representative will act as a liaison between the company and any supervisory authority.

An organisation that is determining whether the GDPR applies to their data processing activities should consider:

- Whether personal data of EU residents is being processed
- Whether personal data is processed within the EU, irrespective of the nationality or location of the data subject.

In the EU Directive, legal obligations were only placed upon data controllers (those organisations that determine the purposes and means of processing personal data). Data controllers can now be held liable for the actions of data processors (those organisations that process personal data on behalf of a data controller). Prior to the GDPR, data processors were only subject to obligations laid down by the controllers through other legal methods such as contractual terms. The GDPR introduces direct legal obligations on data processors, many of which mirror the obligations placed upon data controllers. Data processors should therefore review their resulting risk exposure accordingly.

Even if the GDPR does not apply to an organisation’s processing of personal data, it may apply to the organisation’s customers, suppliers or business partners. They may seek assurances that the organisation’s processing is compliant and may even wish to modify contractual terms to that effect. Therefore, the estimated 2% of Member organisations that the GDPR does not apply to should also consider preparing.

BREXIT

Despite the UK’s decision to leave the EU, tentatively scheduled for 2019, the GDPR will still apply to UK organisations. Once the GDPR comes into effect in 2018, UK organisations will have to comply prior to the UK leaving the EU. Furthermore, even after that time, the GDPR will still apply to any UK organisation processing personal data of EU residents. The UK’s Information Commissioner has stated her intention to align UK data protection laws with the GDPR.
EVALUATE CONTROLS

Unlike the EU Directive, the GDPR mandates that an organisation processing personal data must implement specific people, process, and technical controls. A number of these controls are likely to be of particular significance for an organisation, and key questions should include:

‒ Has a Data Protection Officer been designated, with the appropriate qualifications and powers to manage data protection activities?
‒ Is there a Data Protection Impact Assessment (DPIA) process in place and is it performed on all potentially high risk processing activities and any involving new technologies?
‒ Are ‘data protection by design and default’ principles used in the design of processes and systems?
‒ Is a record maintained of personal data processing activities and the associated security controls used to protect them?
‒ Is personal data transferred to countries outside of the EU and if so, are there suitable legal safeguards to do so?
‒ If there are no offices in the EU, is a representative of the organisation located there?

THE ROLE AND RESPONSIBILITIES OF THE DATA PROTECTION OFFICER

The GDPR defines the requirement for a Data Protection Officer (DPO) in all situations where there is regular or systematic monitoring of data subjects on a ‘large scale,’ or where there is ‘large scale’ processing of special categories of data (previously referred to as ‘sensitive’ personal data, e.g. medical records or criminal history). The Regulation does not define the meaning of ‘large scale,’ but this can be taken as meaning any significant data set, or where the processing is the primary function of the organisation.

By mandating this role, the GDPR creates an information governance function that is independent, capable of reporting its findings to the highest level of management and empowered by the organisation. A DPO is considered by the GDPR to be the organisation’s centre of expertise for the protection of personal data and the GDPR requires that the DPO has expert knowledge of data protection law and practices and the ability to fulfil all of the tasks required by the GDPR. The organisation is responsible for providing resources that allow the DPO to fulfil their tasks, including a reporting line to executive management and sufficient time and funding to maintain their expert knowledge (e.g. through formal training).

Whilst the DPO role will be new for many businesses, it is well established in the public sector and has matured in the US, where companies understand the value of a function that can help protect them from data protection-related incidents.

DATA PROTECTION BY DESIGN AND DEFAULT

The GDPR requires an organisation to adopt appropriate organisational and technical measures (e.g. anonymising personal data) to deliver ‘data protection by design and by default’. The GDPR does not specify these measures, but they are taken to refer to acknowledged Privacy by Design principles2. An organisation will need to ensure that systems and processes include privacy controls and that systems adopt privacy as a ‘default’ setting, for example by automatically opting data subjects out of processing unless they choose to opt in.

RECORD OF PROCESSING ACTIVITIES

The GDPR requires an organisation to maintain a record of processing activities: a detailed register of what personal data is processed, about which categories of data subjects, for what purposes, how and where it is processed, any disclosures of that data, and what security measures are in place to protect it. Supervisory authorities may request these records as part of an inspection or in response to a complaint.

---

DATA PROTECTION IMPACT ASSESSMENTS

Data protection impact assessments (DPIAs) are a key requirement in the GDPR and many organisations may not currently perform them as part of their data processing activities. The GDPR requires that DPIAs are prepared where data processing is likely to pose a high risk to the rights and freedoms of data subjects, particularly when implementing new technologies or during large scale processing of special categories of personal data.

When conducting a DPIA, there are several key elements that the GDPR requires be included, such as a systematic description of the envisaged processing operations and the legal basis for the processing. DPIAs should assess the necessity and proportionality of the processing to determine the risks to the rights and freedoms of the data subjects. Finally, DPIAs should describe the approach that an organisation will take to mitigate the risks, including information regarding the measures taken to ensure the protection of personal data and compliance with the GDPR.

The DPIA should not be an isolated compliance activity, but can instead be embedded in project initiation and change management processes so that potential privacy risks and associated remediation costs are clearly understood during decision-making and approval. Typically, the DPIA approach will include a short ‘screening process’ to identify potential high risk processing activities which may require more detailed scrutiny by the organisation’s DPO, who can then work with the project teams to understand risks and recommend controls.

DATA TRANSFERS

One of the aims of the GDPR is to align EU Member States’ interpretations of data protection law. The EU Directive resulted in varying data protection requirements across the EU, alongside differing levels of effectiveness and regulatory enforcement. This fragmentation ran counter to the EU’s open border policy and the GDPR now acts as a common law across Member States, providing residents with the same level of data protection no matter where their data is processed.

Countries outside of the EU can choose to align their data protection laws and enforcement practices with the EU and hence obtain a decision of ‘adequacy’. Adequacy decisions follow a guiding opinion from the European Data Protection Board (formerly known as the Article 29 Working Party), which is comprised of EU Members States’ supervisory authorities. Once deemed adequate, countries are able to exchange personal data freely with the EU without the need for additional safeguards. Under the outgoing EU Directive, decisions of adequacy have been awarded to countries including Argentina, Canada, New Zealand and Switzerland. The full list of ‘adequate’ countries can be found on the EU’s website.

An organisation requiring the transfer of personal data out of the EU (which can include viewing that data from outside of the EU) needs to ensure that it has a suitable legal basis for doing so. Legal safeguards can include:

– transferring to a third country that is considered to be ‘adequate’
– implementing ‘binding corporate rules’ or EU ‘model contract clauses’ to bind third parties to EU laws and jurisdiction
– registering for the EU-US Privacy Shield
– using ‘explicit consent’ for the transfer.

EU-US PRIVACY SHIELD

The EU-US Privacy Shield defines a mechanism under which personal data can be transferred from the EU to the United States.

A US organisation that receives personal data from the EU under the Privacy Shield or through other mechanisms has to comply with the principles of the GDPR and submit to the powers of EU courts and supervisory authorities for that data.

DESIGNATING A DPO

A DPO does not necessarily have to be a full-time role or require the recruitment of a new employee. The GDPR allows the DPO to be an external party subcontracted for the purposes of fulfilling this role. Equally, a DPO can be employed mutually by multiple organisations. An individual can take on the role of a DPO in addition to other duties, as long as they have the qualifications, resources and reporting lines to meet the requirements of the GDPR.

ASSESS CAPABILITIES

The GDPR includes numerous requirements for an organisation to implement data protection capabilities, without specifying how they are to be achieved, for example having the ability to identify and amend or erase all personal data about an individual. An organisation determining whether it has the capabilities required by the GDPR should ask:

‒ Where consent is the legal basis for processing, is affirmative consent from data subjects collected and documented?

‒ Can evidence of consent be provided for personal data that is already processed?

‒ Are mechanisms in place to identify and erase the personal data of a data subject upon request?

‒ Has a means of providing all personal data relating to a data subject to the subject in a commonly-used, machine-readable format been implemented?

‒ Do incident management plans include the requirement to notify the relevant supervisory authority of a personal data breach without undue delay, and where possible within 72 hours?

‒ Do incident management plans include the requirement to notify data subjects about breaches?

PROCESSING PERSONAL DATA WITH CONSENT AS THE LEGAL BASIS

Consent is the primary method that most organisations use as a lawful basis to process personal data. Under the previous EU Directive, an organisation was able to rely on implicit or ‘opt-out’ consent, allowing it to process personal data unless the data subject requests otherwise. Under the GDPR, however, an organisation should ensure that consent is obtained by means of an affirmative action, rather than through a data subject’s inaction: forgetting to tick a box is no longer considered to be valid consent. This applies to personal data that is already being processed, so an organisation will have to ensure that it can provide documented evidence of consent for all personal data that it processes when using consent as a legal basis, which may be a challenge for many.

Furthermore, consent should be specific to each data processing operation and the request for consent should be: intelligible; easily accessible; clearly distinguishable from other content in a document; and not tied into provision of a service, for example requiring a data subject to agree to receive marketing communications as part of purchasing a product.

The need for consent from children to the processing of their personal data has been under debate for many years and the GDPR mandates that children under the age of 16 cannot consent to their data being processed, instead requiring that their parent or guardian provide consent on their behalf. The GDPR defines prescriptive requirements for privacy notices (often referred to as web privacy policies) and consequently, an organisation should check that the content and usage of its privacy notices reflect GDPR requirements.

RIGHT TO ERASURE

The right to erasure (also known as the ‘right to be forgotten’) is included in the GDPR. Data subjects now have the right to request the erasure of their data from an organisation’s systems without undue delay. This requires not only that current production systems be modified to identify and erase a data subject, but also that business processes prevent the restoration of an erased data subject’s personal data (for example, if data is procured from other sources, restored from backup or retrieved from archives).

RIGHT TO PORTABILITY

The right to portability allows a data subject to obtain their personal data and transfer it to other data controllers. A data subject can request a copy of all personal data relating to them in a format that is structured, commonly used and machine-readable. For companies in commodity markets such as utilities or telecommunications, this could force a significant change to their business model as their customers demand access to their usage data for price comparison purposes.
DUTY TO REPORT PERSONAL DATA BREACHES AND NOTIFY DATA SUBJECTS

Data breach reporting is considered good practice by regulatory bodies and is reflected in some national laws and sector-specific regulations. However, prior to the GDPR, there was no blanket requirement to compel all organisations to report personal data breaches to authorities and affected data subjects.

The GDPR introduces breach reporting to the supervisory authority as a mandatory task, unless the breach is unlikely to result in any risk to the rights and freedoms of the data subjects (that decision being left to the organisation). When reporting to the supervisory authority, a data controller should do so without undue delay and when feasible, should do so within 72 hours after having been made aware of the breach. If it is not reported within 72 hours, the controller should provide reasons as to why this was the case. Breach notifications should include:

- details of the breach
- the types of data
- the number of data subjects affected
- the likely consequences of the breach
- the measures, either taken or proposed, to address the breach.

Data processors now have similar responsibilities for reporting breaches to the supervisory authority, with the exception that there is no time limit on their reporting; they are simply required to report breaches without any undue delay.

Unlike breach reporting to the supervisory authority, breach reporting to data subjects by the data controller is not a task that the GDPR requires should be performed in all scenarios. If a data controller has taken steps post-breach to ensure that high risk scenarios will never appear, or applied measures to make the data unintelligible prior to the breach, then the requirement for breach reporting is not met. However, a supervisory authority may choose to override an organisation’s decisions regarding breach reporting to data subjects.

If the breach is deemed a high risk to the rights and freedoms of the data subjects, then the breach should be reported to data subjects. The report should:

- be provided without undue delay
- be in clear and plain language
- describe the consequences of the breach
- demonstrate the measures taken to address the consequences.

THE VALUE OF CONSENT

Failure to adequately obtain consent can lead to enforcement actions from supervisory authorities. In addition to potential fines, supervisory authorities can block further processing until evidence of consent is provided. For an organisation that relies on consent for its direct marketing activities, this may mean that it is obliged to cease marketing until the issue is resolved.
Like the EU Directive, the GDPR is upheld by national supervisory authorities which monitor the application of the GDPR, protect the fundamental rights and freedoms of data subjects and facilitate the free flow of personal data across the EU. An organisation determining whether it is prepared for the GDPR’s potential impact should ask:

- Are corporate risk registers updated to reflect the potential risks (including fines, suspension of data processing, adverse publicity) arising from failure to prepare for or uphold the GDPR?

The responsibilities of supervisory authorities extend to all organisations based within their territory, as defined by their EU Member State. Each organisation will communicate with a single supervisory authority, known as the lead supervisory authority. This supervisory authority is the body responsible for the territory in which the controller or processor has their main, or only establishment. Whilst other supervisory authorities may raise complaints against an organisation, the organisation should only ever communicate with the lead authority.

In circumstances where an organisation has no establishment in the EU, but processes personal data to which the GDPR applies, the organisation should designate a representative in an EU Member State that contains data subjects whose data the organisation is processing. In appointing this representative, the organisation should empower them to act as a point of contact for data subjects and supervisory authorities. However, they cannot be used as a ‘shield’ against legal actions that may be initiated against the organisation.

Supervisory authorities are granted investigatory powers by the GDPR, allowing them to investigate any complaint that they receive through a variety of measures such as audits, and reviews of certifications and codes of conduct. Complaints may be received not only from the data subjects themselves but also from any organisation or association that chooses to complain or has been chosen by a data subject to represent their interests. These complaints can be submitted to any supervisory authority, not just the supervisory authority with territorial responsibility.

If an organisation is found to be infringing the requirements of the GDPR, supervisory authorities have a variety of corrective powers from which to choose. These include the ability to issue warnings and reprimands to controllers or processors; but also include far more substantial powers, which can compel an organisation to process data in certain manners, or cease processing altogether, as well as force an organisation to communicate data breaches to the affected data subjects.

**THE GDPR AS A BUSINESS OPPORTUNITY**

The GDPR should not be viewed purely as a compliance requirement, as there are potential opportunities arising from implementation. An organisation can use it as an opportunity to improve data quality, revise partnership contracts, relocate processing to more appropriate territories and bring the rigour of the information security function into the data protection function if it is required.
In advance of the GDPR’s enforcement, an organisation should have completed its preparations. In doing so, it should ask:

- Has responsibility and funding for GDPR compliance been assigned?
- Can the skills to achieve GDPR compliance be deployed, developed or recruited?
- Can the requirements of the GDPR be implemented by May 2018?

**DEMONSTRATING COMPLIANCE WITH THIRD PARTIES**

One of the requirements of the GDPR is that a data controller be responsible for the actions of its data processors and should ensure that those data processors have suitable controls in place to handle personal data in accordance with the GDPR. Whether a controller or processor, an organisation should be able to notify partners of requests to rectify or erase personal data, or to restrict or change the purposes of processing. This will require an organisation to review its processing relationships with all third parties and where personal data is shared or transferred, satisfy itself that third party controls and capabilities comply with the GDPR. Similarly, an organisation should expect to have to satisfy those third parties of its own controls.

In practice, an organisation should have completed its GDPR preparations well before May 2018 in order to gain assurance from and provide assurance to third parties’ requests. This will require resources with the expertise and time to issue and process those requests. Data protection, legal and information security teams should plan for this task so that they are not overwhelmed with requests closer to the enforcement deadline.

**DESIGNATING A DATA PROTECTION OFFICER**

The ISF anticipates that most organisations will need to designate a DPO, with the International Association of Privacy Professional’s (IAPP) research suggesting a requirement for up to 75,000 new DPOs worldwide. This likely shortage of qualified individuals, coupled with the length of typical corporate hiring cycles, means that an organisation that has yet to designate a DPO should either start recruitment now; identify an internal candidate and start training them; or seek external expertise to fulfil the role requirements.

**PREPARATION TIMETABLE**

An organisation aiming to comply should conduct preparatory activities as soon as possible to minimise disruption to business operations. The ISF will be providing an Implementation Guide in 2017 to support an organisation’s GDPR implementation efforts.

---

Conclusion

The GDPR is putting data protection practices at the forefront of business agendas worldwide. For most organisations the next 18 months will be a critical time for their data protection regimes as they determine the applicability of the GDPR and the controls and capabilities they will need to manage their compliance and risk obligations.

This Digest has outlined data protection concepts and the changes introduced by the GDPR. It described the foundations of the ISF Approach, highlighting some of the key requirements that an organisation must take into account when preparing its compliance programme, and has set out, at a high level, the initial questions that an organisation should ask to determine the impact that the GDPR will have on it. The ISF Approach recommends that an organisation should:

- determine the applicability of the GDPR to their personal data processing activities
- evaluate control requirements mandated by the new legislation
- assess organisational capabilities to deliver the outcomes required by the GDPR
- understand the financial and operational consequences of non-compliance
- prepare for compliance by 25 May 2018.

Executive management will be responsible for ensuring that an organisation meets its legal obligations to implement the GDPR’s requirements. A DPO should be designated to act as a focal point for ongoing data protection activities. An organisation’s governance functions, including information security, legal, records management and audit should ensure they are familiar with the requirements of the GDPR and have the necessary people, processes and technical solutions in place to achieve compliance.

An organisation aiming to comply should use this Digest in conjunction with the text of the GDPR, found in the EU’s Official Journal. The ISF’s Implementation Guide will be published in the second quarter of 2017 to supplement organisations’ efforts. Together, these publications will enable an organisation to prepare, implement, evaluate and enhance its data protection activities in line with the GDPR’s legal requirements.

WHERE NEXT?
The Compliance community on ISF Live is the place for Members to share and discuss approaches to preparing for and implementing the GDPR. Join this vibrant community to share thoughts, ideas and solutions on the GDPR and learn from other Members’ experiences.

---

Appendix: Glossary of terms

The GDPR contains legal terminology and phrases, and includes definitions of most of the terms used. This glossary provides insight into the terminology used in the Digest.

Data controller
Any natural (e.g. an individual) or legal person (e.g. a company or national body) who is responsible for determining the purposes and means of processing of personal data.

Data processor
Any natural or legal person who processes personal data on behalf of the data controller.

Data subject
A natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, or other data.

EU resident
A natural person who is resident in the European Union.

European Directive
A directive is a legal act of the European Union, which requires Member States to achieve a particular result without dictating the means of achieving that result.

European Regulation
A regulation is a legal act of the European Union which becomes immediately enforceable as law in all Member States simultaneously.

High risk to rights and freedoms
The GDPR does not define a threshold for ‘high risks’ to rights and freedoms, but the level of risk should be evaluated on the basis of an objective assessment. Examples of high risk processing are provided in the GDPR and include the use of new technologies, new kinds of data processing and scenarios in which a data protection impact assessment has never previously been carried out by the data controller.

Large scale
The GDPR does not define ‘large scale’ processing. It is assumed that any organisation processing data of 5,000 or more data subjects performs large scale processing.

Processing
Any operation or set of operations which is performed on personal data, whether or not by automated means, such as (but not limited to) collection, recording, storage, retrieval or destruction.

Reasonable effort
The GDPR does not define ‘reasonable effort’. The term implies that an organisation has taken standard, industry-accepted approaches to achieve a goal, but does not imply that they have performed every available measure.

Rights and freedoms
Fundamental rights provided to all EU citizens by the Charter of Fundamental Rights of the European Union, with the Right to Freedom, (including rights to liberty, privacy and protection of personal data) among the most significant.

Special categories of data
Personal data revealing racial or ethnic origin, medical or criminal records, political opinions, religious or philosophical beliefs, or trade union membership (previously referred to as ‘sensitive’ personal data).

Systematic monitoring
The GDPR does not define ‘systematic monitoring’. The term implies that, due to modern data processing activities, most means of monitoring data subjects is systematic in the current information age.

Undue delay
The GDPR does not define ‘undue delay’ or specify timescales. The term is likely to be based on an opinion of reasonableness that will be applied subjectively from case to case.

---

6 International Association of Privacy Professionals, “Study: At least 28,000 DPOs needed to meet GDPR requirements”. https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/
ABOUT THE ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

WARNING

This document is confidential and is intended for the attention of and use by either organisations that are Members of the Information Security Forum (ISF) or by persons who have purchased it from the ISF direct. If you are not a Member of the ISF or have received this document in error, please destroy it or contact the ISF on info@securityforum.org. Any storage or use of this document by organisations which are not Members of the ISF or who have not validly acquired the report directly from the ISF is not permitted and strictly prohibited. This document has been produced with care and to the best of our ability. However, both the Information Security Forum and the Information Security Forum Limited accept no responsibility for any problems or incidents arising from its use.

CLASSIFICATION

Restricted to ISF Members, ISF Service Providers and non-Members who have acquired the report from the ISF.