



GDPR

A PRACTICAL GUIDE



Get Ready for GDPR

Discover, manage, and protect your GDPR data with Varonis.



Automatically discover and classify GDPR affected data.



Establish access controls and protect regulated data.



Build a GDPR security policy to meet compliance.

The Varonis Data Security Platform gives visibility into our unstructured data locations, who has access and how it is being used. Using this with appropriate policies will allow us to gain full oversight for GDPR.

– Chief Information Security Officer, Non-Profit

Index

EU GDPR Lesson 1 What is the GDPR? Why do we Need it?	4
EU GDPR Lesson 2 Data Protection by Design and by Default	8
EU GDPR Lesson 3 The Right to Be Forgotten	10
EU GDPR Lesson 4 Who is affected by the EU GDPR?	12
EU GDPR Lesson 5 What Happens if I Don't Comply with the EU GDPR?	14
EU GDPR Lesson 6 Next Steps - How to Get There?	16

Get in Touch:

US: +1-877-292-8767 **UK:** +44-203-695-3900 **INTL:** +1-646-706-7336
www.varonis.com

EU GDPR LESSON 1

What is the GDPR? Why do we Need it?

What is the EU General Data Protection Regulation (GDPR)?

The EU GDPR is an evolution of the EU's existing data rules, the Data Protection Directive (DPD). The GDPR is uniform law across the EU and beyond, with new requirements for documenting IT procedures, performing risk assessments, rules on breach notifications, and tighter data minimisation – establishing a single law to enforce European data protection rules and regulation and the right to personal data protection.

It legislates common sense data security ideas, especially from the Privacy by Design school of thought: minimise collection of personal data, delete personal data that's no longer necessary, restrict access, and secure data through its entire lifecycle.

What type of data is protected?

Personal data – or as it's called in the US, personally identifiable information (PII). Think names, addresses, phone numbers, account numbers, and more recently email and IP addresses.

Who does it affect?

The GDPR applies to EU based companies and companies that collect data of EU citizens, regardless of their physical presence in the country.

How does it affect you?

It means there are new regulations and requirements for collecting, recording, and storing personal data and processing activities, new regulations on breach notifications, penalties on violations, and more.

▼ HOW VARONIS HELPS



What are the new requirements?

Privacy by Design – The GDPR has formalised principles of Privacy by Design (PbD) into their regulations including minimising data collection and retention, and gaining consent from consumers when processing data.

Data Protection Impact Assessments (DPIA) – Companies will have to first analyse the risks to their privacy when certain high-risk or sensitive data associated with subjects is to be processed.

Right to Erasure and To Be Forgotten – There's been a long standing requirement in the DPD allowing consumers to request that their data be deleted. The GDPR extends this right to include data published on the web. This remains a controversial right to stay out of the public view and “to be forgotten”.

Extraterritoriality – Even if a company doesn't have a physical presence in the EU but collects data about EU data subjects (through a website, for example) then all the requirements of GDPR are in effect. In other words, the new law will extend outside the EU. This will especially affect e-commerce companies and other cloud-based businesses.

Breach notification – Companies will have to notify data authorities within 72 hours after a breach of personal data has been discovered. Data subjects will also have to be notified but only if the data poses a “high risk to their rights and freedoms”.

Fines – Serious infringements can merit a fine of up to 4% of a company's global revenue. These infringements can include violations of basic principles related to data security – especially PbD principles. A lesser fine of up to 2% of global revenue can be issued if company records are not in order, or if the supervising authority and data subjects are not notified after a breach.

GDPR is a data-centric regulation, so it requires a data-centric security approach. The GDPR highlights that awareness of your data—where is sensitive data stored, who's accessing it, and who should be accessing it— is now more critical than ever.

EU GDPR LESSON 2

Data Protection by Design and by Default

Privacy by Design (PbD) is a well-intentioned set of principles to get the C-suite to take consumer data privacy and security more seriously. Overall, PbD is a good idea and you should try to abide by it.

But with the General Data Protection Regulation (GDPR), it's more than that: it's the law if you do business in the EU!

PbD dispenses good general advice on data security that can be summarised in one word: minimise.

Minimise collection of consumer data, minimise who you share the data with, and minimise how long you keep it. Less is more: less data for the hacker to take means a more secure environment.

It's not too much of a stretch to say that if you implement PbD, you're well on your way to mastering the GDPR.

So can big data and privacy live together happily ever after? Privacy by Design (PbD) says yes – with just a few basic steps, you can achieve the PbD vision:



Minimise data collected (especially PII) from consumers.



Do not retain personal data beyond its original purpose



Give consumers access and ownership of their data

EU GDPR LESSON 3

The Right to Be Forgotten

The controversial “*right to be forgotten*” is now law in the EU.

For most companies, this is really a right for consumers to erase their data.

The GDPR has strengthened the DPD’s existing rules on deletion and then adds the right to be forgotten. There’s now language that would force the controller to take reasonable steps to inform third-parties of a request to have information deleted.

Discussed in **Article 17** of the GDPR, it states that “*The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where ... the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; ... the data subject withdraws consent on which the processing is based ... the controller has made the personal data public and is obliged ... to erase the personal data*”.

This means that in the case of a social media service that publishes personal data to the Web, they would have to remove not only the initial information, but also contact other web sites that may have copied the information. This would not be an easy process!

What if the data controller gives the personal data to other third-parties, say a cloud-based service for storage or processing?

The long arm of the EU regulations still applies: as data processors, that cloud service will also have to erase the personal data when asked to by the controller.

Translation: the consumer or data subject can request to erase the data held by companies at any time. In the EU, the data belongs to the people!

EU GDPR LESSON 4

Who is affected by the EU GDPR?

One of the more complex issues with the new GDPR is what's being called "extraterritoriality." Under **Article 3**, the GDPR will apply to any personal data transferred outside the EU.

So under these new rules, if a US company collects data from EU citizens, it will be under the same legal obligations as though the company had headquarters in say France, UK, or Germany — even though they don't have any servers or offices there!

Legal experts note this may not be that easy to enforce, but if a large enough multinational breaks one of the rules — such as the GDPR's new strict breach notification requirement — it is likely that the EU regulators will target it.

Obviously, extraterritoriality is particularly relevant to core web services such as search, social networking, e-commerce, companies that allow you to rent apartments online, etc.

You can map these to your own favourite apps to figure out who would be affected.

Shifting Meanings

Under the old rules in the Data Protection Directive (DPD), there was some wiggle room that allowed data collectors to escape having to follow the regulations. A common practice was for service or app providers to keep their data processing outside the EU.

The idea was that if the main processing and servers weren't located in the EU zone, then the rules didn't apply.

Companies such as Google, Facebook, and other social networking companies were following this approach.

Not so fast!

Google was famously making this argument when a Spanish DPA asked it to remove a listing in a search result. The case eventually made its way to the EU's highest court, the ECJ, which ruled against Google.

The long arm of EU law prevailed: the specific search listing was removed.

This idea of extended territorial scope is made explicit in the GDPR's **Article 3**. The GDPR will apply to EU based companies and companies that collect data of EU citizens, regardless of a physical presence in the EU.

EU GDPR LESSON 5

What Happens if I Don't Comply with the EU GDPR?

The GDPR has a tiered penalty structure that will take a large bite out of offenders' funds – and GDPR rules apply to both data controllers and processors: therefore huge cloud providers are not off the hook when it comes to GDPR enforcement.

Non-compliance results in fines of up to 4% of global revenue.

A company can be fined up to 2% of global revenue for not having their records in order (**article 30**), not notifying the supervising authority and data subject about a breach (**articles 33, 34**), or not conducting impact assessments (**article 35**).

And keep in mind, the GDPR breach notification requires more than just saying you have had an incident. You'll have to include categories of data, records touched, and approximate number of data subjects affected.

This means you'll need some detailed intelligence on what the hackers and insiders were doing.

More serious infringements merit up to a 4% fine of global revenue. These infringements include violations of basic principles related to data security (**article 5**) and conditions for consumer consent (**article 7**) – violations of the core Privacy by Design concepts of the law.

One way the GDPR regulators are hoping to keep everything in line is by requiring companies to have a Data Protection Officer (DPO). The DPO should be responsible for creating access controls, reducing risk, ensuring compliance, responding to requests, reporting breaches within 72 hours, and creating a strong data security policy.

EU GDPR LESSON 6

Next Steps - How to Get There?

Article 25

Data Protection by Design and By Default

WHAT IT MEANS

Embrace accountability and privacy by design as a business culture.

HOW VARONIS HELPS

Identify who has access and who should have access to regulated data; manage permissions; automatically remediate risks like global group access and inconsistent ACLs; get to a least privilege model.

Article 30

Records of Processing Activities

WHAT IT MEANS

Implement technical and organisational measures to properly process personal data.

HOW VARONIS HELPS

Identify, discover, and classify sensitive and GDPR eligible data; monitor, analyse, and report on user activity on that data; establish and automate data retention policies; conduct data security reviews and generate reports based on type of data, access activity, and more.

Article 17

Right to Erasure and “to be forgotten”

WHAT IT MEANS

Be able to discover and target specific data and automate removal.

HOW VARONIS HELPS

Identify, discover, and classify sensitive and GDPR eligible data; establish and automate data retention policies. Configure end-to-end migration rules based on defined criteria to allow for the rapid and safe execution of complex data migrations, and to easily implement and enforce policies for data retention or deletion.

Article 32

Security of Processing

WHAT IT MEANS

Ensure least privilege access; implement accountability via data owners; provide reports that policies and processes are in place and successful.

HOW VARONIS HELPS

Reduce risk and manage access controls: automate and impose least privilege with entitlement reviews and proactively enforced ethical walls and security policies.

Article 33

Notification of personal data breach to the supervisory authority

WHAT IT MEANS

Prevent and alert on data breach activity; have an incidence response plan in place.

HOW VARONIS HELPS

Alert on suspicious behaviour and potential data leaks; detect data breach and malware activity; monitor policy violations.

Article 35

Data Protection Impact Assessment

WHAT IT MEANS

Quantify data protection risk profiles.

HOW VARONIS HELPS

Monitor and assess your state of data protection and security with a data risk assessment: identify and lock down sensitive data, analyse accounts with suspicious behaviour, detect malware activity, and more.

So what should you focus on to meet the EU General Data Protection Regulation?

Data classification – Know where personal data is stored on your system, especially in unstructured formats in documents, presentations, and spreadsheets. This is critical for both protecting the data and also following through on requests to correct and erase personal data.

Metadata – With its requirements for limiting data retention, you'll need basic information on when the data was collected, why it was collected, and its purpose. Personal data residing in IT systems should be periodically reviewed to see whether it needs to be saved for the future.

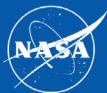
Governance – GDPR highlights the need to get back to basics. For enterprise data, this should include understanding who is accessing personal data in the corporate file system, who should be authorised to access, and limiting file permission based on employees' actual roles – i.e., role-based access controls.

Monitoring – The breach notification requirement places a new burden on data controllers. Under the GDPR, the IT security mantra should be “always be monitoring”. You'll need to spot unusual access patterns against files containing personal data, and promptly report an exposure to the local data authority. Failure to do so can lead to enormous fines, particularly for multinationals with large global revenues.

Varonis helps companies meet GDPR compliance requirements: automatically discover and classify GDPR data with over 250 exclusive patterns to identify GDPR eligible data, monitor and alert on suspicious behaviour and unusual activity, establish access controls and data protection policies, and build a unified data security strategy to protect customer data.

Varonis is a pioneer in data security and analytics, specialising in software for data security, governance, compliance, classification, and analytics. Varonis detects insider threats and cyberattacks by analysing file activity and user behaviour; prevents disaster by locking down sensitive data; and efficiently sustains a secure state with automation.

We help thousands of customers prevent data breaches.



Get a GDPR Readiness Assessment



Data Risk Assessment

Get your risk profile, discover where you're vulnerable, and fix real security issues.

varonis.com/gdpr-ra



Live Demo

Set up Varonis in your own environment and see how to stop ransomware and protect your data.

info.varonis.com/demo

