Elavon

Get ready

A Guide to the General Data Protection Regulation (GDPR)

elavon.ie

The General Data Protection Regulation (GDPR) will regulate the privacy and handling of the personal data of individuals in the European Union (EU). This guide explains what it means, how it'll impact individuals and businesses like yours and tells you everything you need to know about the new law.

GDPR summary

When does the new regulation start?

25 May 2018

What's new?

There are new rights for people to access the information companies hold about them, obligations for better data management for businesses, and a new regime of fines

What is GDPR?

In January 2012, the European Commission set out plans for data protection reform across the European Union in order to make Europe ‘fit for the digital age’. Almost four years later, agreement was reached on what that involved and how it will be enforced.

One of the key components of the reforms is the introduction of the General Data Protection Regulation. This new EU framework applies to organisations in all member-states and for global businesses that do business with individuals in the EU.

At its core, GDPR is a new set of rules designed to give people more control over their data. It aims to simplify the regulatory environment for business so both people and businesses can fully benefit from the digital economy.

The reforms are designed to reflect the world we’re living in now, and brings laws and obligations across Europe up to speed for the internet-connected age.

Fundamentally, almost every aspect of our lives revolves around data. From social media companies, to banks, retailers, and governments - almost every service we use involves the collection and analysis of our personal data. Your name, address, payment card number and more are all collected, analysed and, perhaps most importantly, stored by organisations. The GDPR aims to harmonise regulation across Europe to reflect today’s data exchange landscape.

What does it mean to my organisation?

The GDPR will apply to an organisation or person that handles any personal data of people in the EU. This means that companies and individuals based outside the EU that sell goods and services to individuals living in the EU will also need to comply with the new law. That ultimately means that almost every major corporation in the world will need to be ready when GDPR comes into effect, and must start working on their GDPR compliance strategy. The GDPR applies to controllers, joint controllers and processors, but the distinction is important as the obligations for each differ.

Are you a controller or a processor?

The different terms

Not everyone that handles the personal data of individuals is the same and data protection laws allow for this by having three different categories: Controller, Joint Controller and Processor. Here's what they mean:

Controller

A controller is the entity (a person or a company) that determines the purpose and means of processing personal data.

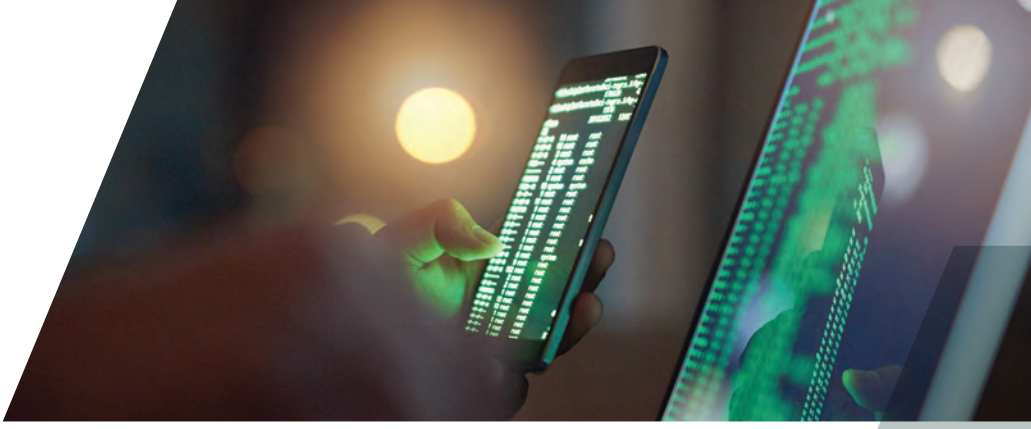
Joint controller

Where two or more companies jointly determine the purposes and means for the processing of personal data e.g. they jointly decide the purposes/ reasons, occasion, nature and scope and objectives of the processing.

Processor

The person or group that processes the data on behalf of the controller. Processing is obtaining, recording, adapting or holding personal data.

The same entity can be both a controller and a processor, depending on the circumstances. For example, a technology company that provides payment processing technology to online merchants is the processor and the merchant is the controller. However, if that technology company packages the same personal data to provide targeted customer segments to advertisers, it is acting as a controller.



GDPR ultimately places legal obligations on a processor to maintain records of personal data and how it is processed, providing a much higher level of legal liability should the organisation be breached.

Controllers will also be forced to ensure that all contracts with Data Processors comply with GDPR.

What is personal data and sensitive personal data?

The types of data considered personal under the existing legislation include name, address, and photos. GDPR extends the definition of personal data so that, in certain circumstances, something like an IP address can be personal data. It also includes sensitive personal data such as genetic data, and biometric data which could be processed to uniquely identify an individual.

Personal data

Data which relates to a living individual who can be identified directly or indirectly, e.g.:

- Name
- Phone number
- Email address
- Payment card number

Sensitive personal data

Personal data consisting of information such as:

- Racial or ethnic origin of the data subject
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Whether a member of a trade union
- Physical or mental health or condition
- Sexual life

What the GDPR sets out

There are 99 articles within the GDPR. These range from general provisions, responsibilities of the controller, joint controller and processor, to cooperation with the supervisory authority.

Key changes that may impact your organisation include:

- **Privacy-by-design** – Data protection must be built into business processes and systems from the start and provided by default
- **Right to be forgotten** – Users can request for their data to be deleted; they can also request for a copy to be sent to a third party
- **Mandatory breach notification** – Certain breaches of personal data must now be reported to authorities within 72 hours and to affected individuals without delay
- **Penalties for non-compliance** – GDPR allows for fines of up to €20 million or 4% of the company's annual global turnover, whichever is the greater

What does GDPR compliance look like?

There's no 'one size fits all' approach to preparing for GDPR.

Each business will need to examine what exactly needs to be achieved to comply. It's important to understand whether you are a data processor or a data controller. Most companies are likely to be both depending on the specific data you receive.

How to prepare

- Start by getting an understanding of what personal data is being held and who has access to it
- Limit access based on business need and implement monitoring to detect any unauthorised access
- Perform an assessment of what compliance and security controls you have in place to collect and protect the data, how effective they are, and where the gaps are
- Develop a plan to improve your security program, looking at people, process and technology
- Put in place a data breach notification process, including incident detection and response capabilities
- Some organisations must also have a Data Protection Officer (DPO)

The PCI DSS framework supports GDPR security compliance

The GDPR does not set out in detail a compliance/security framework. However, the Payment Card Industry Data Security Standards (PCI DSS) provides a useful starting point for a personal data management compliance program. Replacing one word, (from 'cardholder' to 'personal' data) within the 12 main requirements for PCI DSS will provide a logical structure 'payment' to 'personal' to approach GDPR security compliance:

Goals	Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect **personal** data 2. Do not use vendor-supplied defaults for system passwords and other security parameter
Protect cardholder data	3. Protect stored **personal** data 4. Encrypt transmission of **personal** data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to **personal** data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to **personal** data
Regularly monitor and test networks	10. Track and monitor all access to network resources and **personal** data 11. Regularly test security systems and processes
Maintain an Information security policy	12. Maintain a policy that addresses information security for all personnel

If you are PCI DSS compliant and you treat all your personal/important data the same way as you treat cardholder data you're well on your way. Importantly, PCI DSS does not cover everything set out by the GDPR, but provides a useful starting point to address data security (Article 32 EU GDPR - 'Security Processing').

Preparation checklist for GDPR compliance

- ☐ Establish a programme of work to gather a coherent inventory of your processes that relate to personal data.
- ☐ Have a process by which you risk-assess your own data.
- ☐ Have an understanding of where and how you share personal data with third parties, and ensure that you have the correct contracts in place to comply with GDPR.
- ☐ Assess your information security program as it relates to personal data, including third parties you share data with.
- ☐ Be compliant with the Payment Card Industry Data Security Standard (PCI DSS) for baseline security around personal and cardholder data.
- ☐ If applicable, ensure the information and the consent language you provide to your customers is transparent, clear, unambiguous, and written in plain language.
- ☐ Outline a plan for compliance with the more complex rights of the data subject, including rights of access, rights of correction, rights of rectification, rights of data portability, and rights of erasure.
- ☐ Establish a mechanism to identify if, when, and where any breach takes place and how you will handle it.
- ☐ Have a PCI Forensic Investigator (PFI) on retainer for the event of a card data breach.

What are the implications of non-compliance?

Companies that have not taken steps to ensure their personal data processing activities fulfil their new obligations under GDPR, could be liable for fines in relation to non-compliance. These fines can be imposed on both data controllers and data processors.

Failure to comply with GDPR can result in a fine of up to €20 million or 4% of the parent company's annual global turnover, a figure which for some could mean millions or going out of business.

Fines will depend on the severity of the breach and on whether the company is deemed to have taken compliance and regulations around security in a serious enough manner.

The maximum fine of €20 million or 4% of worldwide turnover, whichever is greater, is for infringements of the rights of the data subjects, unauthorised international transfer of personal data, and failure to put procedures in place for or ignoring subject access requests for their data.

The lower limit of €10 million or 2% of worldwide turnover will be applied to companies which mishandle data in other ways. They include, but aren't limited to, failure to report a data breach, failure to build in privacy by design and ensure data protection is applied in the first stage of a project and be compliant by appointing a Data Protection Officer (if applicable).

How can Elavon help?

Questions you may be tackling:

- How do we get consent from employees?
- What exactly should I be recording in relation to processing activities?
- Are we the data controller for employee information we pass on to pension and health benefit providers?
- How does PCI DSS fit into all this and does it help?
- Do we need a Data Protection Officer (DPO)?
- What do we do with all our marketing data?

To help customers deal with these queries, Elavon has established relationships with a number of leading data security firms. Together with our partners, Elavon can help you address all your PCI and GDPR questions, with services ranging from audit, consultancy, gap analysis and incident readiness planning to managed security services.

Contact us now on **PCIEurope@elavon.com** for more information.

Let's work together

Contact us to see how we can assist you with your preparations to comply with PCI DSS and the GDPR.

We make it possible. You make it happen.

PCIEurope@elavon.com

elavon.ie/security

Y2719v20318