Grant Thornton

An instinct for growth™

Risk

Regulation

Cyber security

# The General Data Protection Regulation (GDPR)

## Preparing your business for the GDPR

**September 2017**

# Contents



# What is the GDPR and what does it change?

The General Data Protection Regulation (GDPR) is the European Union's (EU) new data protection law that comes into effect on 25 May 2018.

Implemented throughout the EU, it will govern all businesses operating within the union and embed a more consistent approach to data protection. Companies that trade with EU-based businesses will also be impacted and will need to know what's changing and how to comply.

**Penalties for non-compliance can now be up to €20 million or 4% of annual global turnover – whichever is greater.**

## So why is data protection legislation transforming?

Since 1995, the Data Protection Directive (Directive 95/46/EC) has determined how individuals' personal data is protected within the EU. However, since its inception there have been vast developments in the sophistication and scale of data creation and gathering – for example through the emergence of social media, cloud computing and geolocation services. As the directive predates these developments, it's no longer suitable to govern the current data landscape; it needs to be refreshed to address modern privacy concerns and facilitate consistency across the EU. This is what the GDPR will do.

The new regulation introduces a huge range of changes. Underlying this shift is the EU's ongoing agenda to safeguard its citizens and their private information. The GDPR will establish new rights for individuals and strengthen current protections by applying stricter requirements to the way businesses use personal data. If they fail to comply, the sanctions will be significantly larger.

## What this means for your business

The GDPR is a valuable opportunity to understand your business's data and use it more effectively. However, it requires strict adherence to the new regulation and a clear understanding of the changes in order to avoid large penalties.

First, it's critical to be aware that the GDPR supersedes all existing data protection acts, and that it increases businesses' obligations around data protection and their accountability for failure. It also applies across the full spectrum of data engagement – from the collection of personal data through to its use and disposal. Your organisation will need to embed policies and procedures to ensure that it monitors its GDPR controls and documents its compliance.

The new rules apply to organisations of any size that process personal data. Whatever the nature of your organisation, the GDPR will have a substantial impact. As its implementation date is getting closer, early preparation is key.

**All global organisations, both those in the EU and those that trade with EU companies, will be required to comply with the GDPR from May 2018.**

# Understanding the core changes

The GDPR will introduce wide-ranging changes that require thorough understanding, internal stakeholder acceptance, appropriate preparation and implementation across the whole business. To provide an overview, we've addressed some of the key changes here.

**Better rights for data subjects**
The largest shift is that individuals will benefit from greatly enhanced rights, for example, the right to object to certain types of profiling and automated decision-making. Consent requirements will also be more stringent. Consent must be explicit and affirmative, it must be given for a specific purpose and it must be easy to retract. Individuals can also request that personal data is deleted or removed if there isn't a persuasive reason for its continued processing.

**Increased accountability**
Organisations will have far more responsibility and obligation. They will need to publish more detailed fair processing notices – informing individuals of their data protection rights, explaining how their information is being used and specifying for how long. The new regulation also embeds the concept of privacy by design, meaning organisations must design data protection into new business processes and systems.

**Formal risk management processes**
Organisations must formally identify emerging privacy risks, particularly those associated with new projects, or where there are significant data processing activities. They must also maintain registers of their processing activities and create internal inventories. For high-risk data processing activities, Data Protection Impact Assessments (DPIAs) will be mandatory. It will also be compulsory to appoint a Data Protection Officer (DPO).

**Reporting data breaches**
As part of the drive for greater accountability, data breach reporting is becoming stricter. If a significant data breach occurs, it must be reported to the Data Protection Commissioner within 72 hours and, in some cases, to the individual affected without undue delay.

**Significant sanctions**
Penalties for non-compliance with the GDPR will rise considerably, up to €10 million or 2% of annual global turnover (whichever is greater) for minor or technical breaches, and €20 million or 4% of turnover for more serious operational failures.

**Data processing requirements**
The regulation also imposes new requirements on data processors, and includes elements that should be addressed contractually between data processors and data controllers.



## Key features of the GDPR:

**Enhanced rights for data subjects** – the right to object to certain types of profiling and automated decision-making, and to request that unnecessary personal data is deleted.

**Privacy by design** – organisations must design data protection into new and existing business processes and systems.

**Enhanced obligations for organisations** – such as publishing detailed fair processing notices to inform individuals of their data protection rights, the way their information is used and for how long.

**Increased record keeping** – organisations must maintain registers of the processing activities they carry out, with mandatory DPIAs for high-risk data processing.

**Stringent consent requirements** – consent must be explicit, freely given for a specific purpose and easy to retract.

**Significant penalties** – the potential size of fines for non-compliance will be considerable, reaching €20million or up to 4% of turnover, whichever is greater.

**Stricter breach reporting** – significant data breaches must be reported to regulators within 72 hours and sometimes the individual, too.

**Appointing DPOs** – appointing a data protection officer will be mandatory for many organisations.

**Increased privacy impact assessments** – organisations must formally identify emerging privacy risks, particularly for new projects.

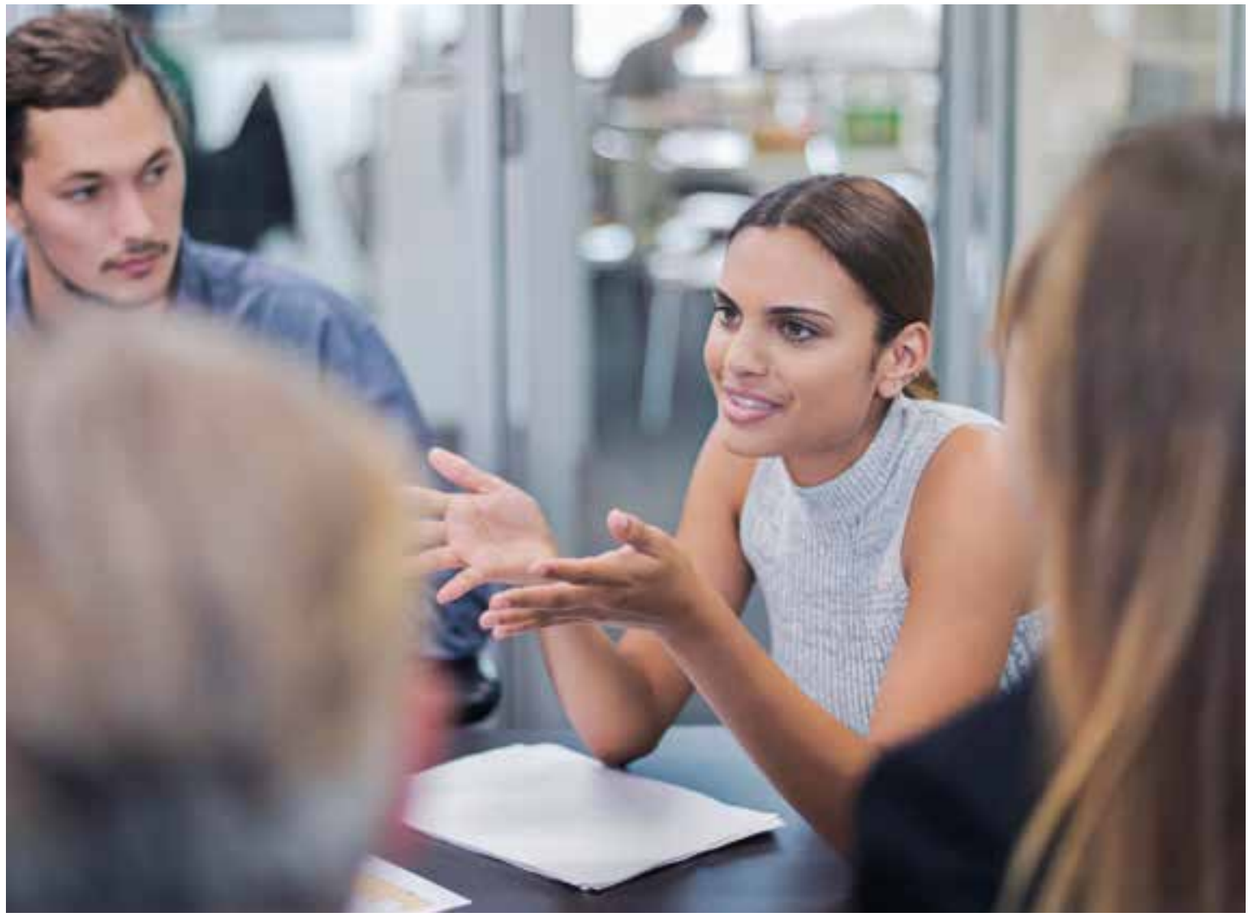
**Wider regulatory scope** – the new regulation will apply to both the data controller and the processor.

# How to prepare your business

The legal landscape of data protection is evolving rapidly, and presenting challenges for businesses, government and public authorities. If your organisation is consumer-facing, online, in the financial services sector or in possession of sensitive personal data it may be particularly affected.

With the deadline growing closer, you'll need to scrutinise the regulatory changes and understand how they will affect your business operations. Bear in mind that the impact of GDPR isn't confined to a specific area of your business – it will require business-wide adoption of a more process-orientated approach.

It's likely you'll need to amend your business practices to become compliant with this new regulation, and implement new controls. So where should you start? We've created a simple visual, below, to help structure your approach to achieve compliance.



### GDPR

- Understand the key changes this legislation will bring

### Data protection quick check

- Assess your organisation's current data architecture, processes, and risk and compliance controls

### Audit results and analysis

- Identify the current data risks in your business
- Review how ready your business is for the GDPR

### Implementation roadmap

- Develop an implementation roadmap that embeds suitable regulatory and compliance architecture
- Ensure the plan is realistic and achievable for your organisation

### Implementation

- Appoint a trusted advisor to:
  - identify and document data processing activities
  - carry out data impact assessments
  - develop a data breach response action plan
  - implement ongoing data protection processes.
- Write a detailed data protection policy and define a standard that ensures your business will meet the GDPR
- Where necessary, appoint a data protection officer and/or a data protection management system for ongoing control

### Measure data protection effectiveness

- Undertake a GDPR FIT/GAP analysis or ISO 27001 FIT/GAP analysis – this is an assessment of the effectiveness of your GDPR efforts

### Continuous improvement

- Hold regular GDPR audits and Data Privacy Impact Assessments
- Ensure data risk management is integrated into your overall risk management structure
- Regularly review your organisation's data protection training needs

# Contact us

To discuss how we can help your business understand its GDPR requirements and become compliant with the new regulation, get in touch with one of our member firm specialists.


**Georg Beham**
Partner, Grant Thornton, Austria
georg.beham@at.gt.com

**Jean de Laforcade**
Associate, Grant Thornton, France
jean.delaforcade@fr.gt.com

**Derek Han**
Partner, Grant Thornton, US
derek.han@us.gt.com

**Mike Harris**
Partner, Grant Thornton, Ireland
mike.harris@ie.gt.com

**Alessandro Leone**
Partner, Bernoni Grant Thornton, Italy
alessandro.leone@bgt.it.gt.com

**Manu Sharma**
Partner, Grant Thornton, UK
manu.sharma@uk.gt.com

**Bjorn Roskott**
Senior IT audit manager,
Grant Thornton, Netherlands
bjorn.roskott@nl.gt.com


Grant Thornton
An instinct for growth™

**grantthornton.global**




EPI.172