The GDPR

- Are you ready for the road ahead?

In 2016, the EU adopted the **General Data Protection Regulation (GDPR)**, replacing the 1995 Data Protection Directive. The European Commission has said that **90% of Europeans** say they want the same data protection rights across the EU, regardless of where their data is processed. The **reform of EU data protection rules** mean people have more control over their personal data and **businesses benefit** from a level playing field.

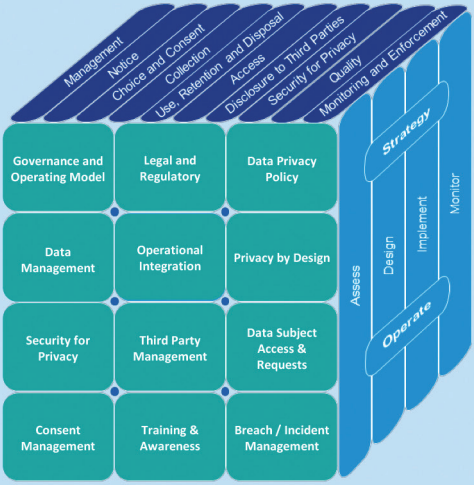
These changes, which came into effect in **May 2018,** reflect an increased focus by the European Commission on data protection. The GDPR means **one set of rules** for all companies operating **in the EU**, wherever they are based. The following steps outline some of the key areas you should consider to help **you prepare for the road ahead.**

1. Can you demonstrate Accountability?

- It's not enough to say that you are GDPR compliant. You must be able to prove it.
- The Accountability principle makes businesses responsible for demonstrating compliance with the GDPR.
- Businesses must have confidence in their Data Protection Strategy in order to be able to demonstrate Accountability.

Do your data and privacy processes demonstrate accountability?

- KPMG's Privacy Management Framework addresses GDPR articles by design. It covers the twelve main categories covered by the data protection regulations and analyses your control framework.
- Following this enables you to adopt a risk-based and pragmatic approach to achieve your goals.



2. Can you respond to a Data Breach?

- Breach notifications are now mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals".
- Data controllers are required to report breaches to the relevant supervisory authority, where the breach presents a risk to the affected individuals.
- Data processors are also required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.
- A loss of personal data can cause severe reputational damage, potentially leading to a loss of customer trust.

What should you consider?

- Are you able to detect, investigate, report and document any breaches?
- KPMG experts have developed breach management solutions to manage, report and minimise the impact of data breaches.

3. Do you maintain sufficient Records of Processing?

- The GDPR makes it necessary for businesses to maintain a record of all processing of personal data.
- Businesses must record how and what types of personal data is captured, stored and processed.

How can KPMG support you?

- KPMG can support the creation and management of records of personal data processing activities.
- Our teams work with businesses to create consolidated Personal Data Registers.
- Personal Data Registers should be created and maintained for every business to effectively manage personal data and can be used to demonstrate GDPR compliance.

4. Are your Third Party Processors and Joint Controllers prepared?

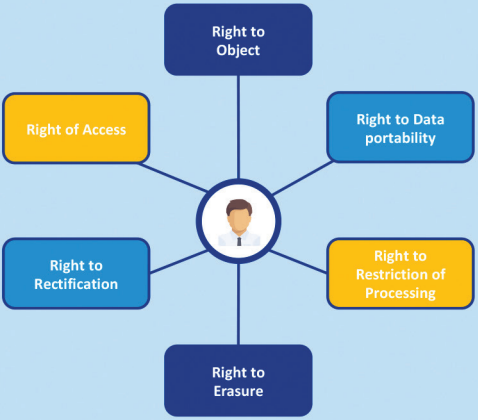
- The GDPR requires your third party processors and joint controllers to be compliant.
- Businesses are required to review all contractual arrangements to understand where Personal Data is shared and stored and whether this data is ever transferred outside of the European Union.

How can KPMG help assess your third party processors and joint controllers?

- KPMG have developed a Data Processor Assessment Model to analyse and evaluate your business' Third Party Processors and Joint Controllers.
- Our Model has been specifically designed to assess 'Organisational and Technical' security measures against six different domains of measurement, including data and privacy management.

5. Are you aware of the Data Subjects rights?

- The GDPR gives Data Subjects several more rights, and therefore gives businesses additional responsibility when it comes to the processing of Personal Data.
- Firms should have Policies and Procedures outlining how to manage data requests.



How can KPMG help?

- KPMG can offer a technology enabled solution to meet your needs, increasing the efficiency for your business in managing and responding to Data Subjects rights requests.
- KPMG provides solutions that supports key Data Subject Request activities, importantly integrating with your existing processes and technologies to increase efficiencies in responding to requests.

6. Are you safe from an attack on personal data?

- The GDPR requires businesses to build data protection safeguards into their products and services from the earliest stages of development.
- By implementing appropriate safeguards and controls, data protection comes by default.

Are your safeguards and controls robust?

- KPMG's safeguard and control assessment helps businesses to identify gaps, risks and pinpoint areas of vulnerability within your business.
- Our teams create solutions to minimise risks as well as working with the business to implement these controls.

7. Do you need to complete Data Protection Impact Assessments?

- The GDPR introduces a new obligation to conduct a Data Protection Impact Assessment (DPIA) before carrying out new processing activities.
- The DPIA is a key element of the new focus on accountability and data privacy by design and default.
- It helps businesses to identify and address the data protection risks of any new processing activities undertaken.

Should you carry out DPIAs?

- A DPIA is required if processing is likely to result in a high risk to individuals' rights and freedoms.
- A DPIA is not required for every process. KPMG help businesses to assess if a DPIA is required.
- KPMG offers deep expertise and support to businesses through the process of completing DPIAs, and assessing the effectiveness of privacy controls.

8. Have you prepared your employees?

- Without data privacy training, there is a risk that employees may not handle personal data in line with the regulations.
- Employees must be prepared, fully equipped and aware of data protection practices within your business.

How can you prepare your employees?

- KPMG offer training and awareness to enable employees to become familiar with Data Protection Laws and create a culture of data protection within the everyday business environment.
- KMPG can provide executive briefings on data protection, classroom-based training and online training.
- Our teams have experience in cultural change and transformation and can help make data protection a high priority issue in your organisation.

9. What is the cost of non – compliance?

- Your local Data Protection Authority monitors compliance; their work is coordinated at EU-level.
- Infringements of the GDPR can lead to fines of different levels depending on which provisions are infringed.
- At the lower level this can be up to €10 million or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Or at the higher level up to €20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

GDPR

These changes aim to provide all EU citizens with more control over their data and protection from privacy and data breaches. The European Commission has said the regulation is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market.

Contact Us

Please call us if you would like to discuss the most efficient and compliant implementation processes to suit your needs.

Michael Daughton
Partner
T: +353 1 410 2965
E: michael.daughton@kpmg.ie

Paul Toner
Partner
T: +353 1 410 1277
E: paul.toner@kpmg.ie

Cormac Deady
Director
T: +353 1 700 4050
E: cormac.deady@kpmg.ie

Tom Hyland
Associate Director
T: +353 1 700 4223
E: tom.hyland@kpmg.ie

kpmg.ie

This document is made by KPMG in Ireland, an Irish partnership and a member firm of the KPMG network of independent firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity, and is in all respects subject to the negotiation, agreement, and signing of a specific engagement letter or contract. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

© 2019 KPMG, an Irish partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks of KPMG International Cooperative ("KPMG International"), a Swiss entity. (4750)