Grant Thornton

An instinct for growth™

The General Data Protection Regulation (GDPR)

Meeting the new requirements

Data protection rules are changing

Over the last 20 years the Data Protection Act (DPA) has been the foundation for protecting privacy in the UK. Predating social media, cloud computing and geolocation services, the law needs to be refreshed to address modern privacy concerns. The EU General Data Protection Regulation aims to do just that.

The GDPR offers a consistent approach to data protection across all EU member states. It aims to increase organisational accountability for all aspects of data protection, from the collection of personal data to its disposal.

The key features of the GDPR include:

- Enhanced rights for individuals – including the right to object to certain types of profiling and automated decision making
- Obligations on organisations to publish more detailed fair processing notices – informing individuals of their data protection rights, how their information is being used and for how long
- Stringent consent requirements – consent must be explicit and freely given for a specific purpose, and must be easy to retract
- Data processors – new requirements are imposed on data processors, including elements which should be addressed contractually between them and data controllers
- Breach reporting – significant data breaches must be reported to regulators within 72 hours
- Privacy impact assessments – organisations must formally identify emerging privacy risks, particularly those associated with new projects
- Privacy by design – organisations must design data protection into new business processes and systems
- Record keeping – organisations must maintain registers of the processing activities that is carried out

Who's affected?

All organisations processing personal data will be required to comply with the GDPR from May 2018.

What about Brexit?

The GDPR comes into effect in May 2018. It applies to all organisations processing the personal data of individuals in the EU, regardless of where that organisation is based. Following Brexit, UK organisations processing the personal data of individuals in the EU will still need to be compliant with the GDPR. It is anticipated that UK data protection laws post-Brexit will be broadly in line with the GDPR.

Data Protection Officers (DPO)

Many organisations will be required to appoint a DPO, including:

- All public bodies processing personal data, including local authorities and schools.
- Organisations which, as a core part of their business, monitor individuals on a consistent and large scale. This includes companies collecting large amounts of data from connected devices, loyalty programmes or CCTV.
- Companies processing large amounts of special categories of personal data, such as race, health or religion.

Data Protection Officers must be appropriately experienced and independently minded. They cannot also hold conflicting roles, such as the CEO, CFO or Head of IT.

New accountability requirements

The regulation seeks to improve accountability for data protection. Organisations must establish a culture of monitoring their GDPR controls and documenting their compliance.

Audit and monitoring requirements

Organisations must document their processing activities in order to demonstrate compliance with data protection principles. The records should:

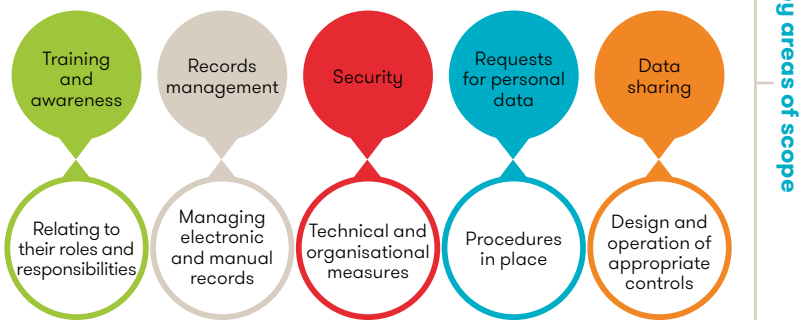
- contain a general description of the technical and organisational security measures protecting personal information
- include a process to regularly test, assess and evaluate the effectiveness of these measures
- be kept in a form that can be used as evidence of compliance
- be made available to the Information Commissioner's Office (ICO) on request.

ICO audits

The ICO conducts audits to assess the arrangements that organisations have in place to comply with privacy laws. They are broken down into key areas of scope as illustrated below:

Accountability

Providing assurance to senior management that effective data protection governance controls are in place to ensure compliance



Every scope area will have a number of controls in place, each of which will be given a specific score. Where risks are identified, the ICO will make recommendations for increased assurance.

What are the risks of non-compliance?

Under the DPA, ICO fines are capped at £500,000. The GDPR, raises the cap to €20 million or 4% of global turnover – whichever is higher.

In practice, this means organisations will be under greater pressure to provide assurance to their boards, customers and regulators that their data protection processes are robust and fit for purpose.

What should be done?

Organisations need to know how the GDPR affects them. They need to assess their current processes and establish which business areas will be impacted and how. By May 2018, they should have:

- evidence of GDPR readiness for their internal stakeholders, internal audit and regulators
- clarity on how the risks to personal data have been understood and embedded within the business
- new or updated data protection policies, processes, procedures and controls fully embedded
- governance documentation produced and available for inspection.

How we can help

We understand the regulation and what it means for you. Our subject matter experts have extensive industry experience, across all aspects of risk and resilience management. We know how to find solutions which work for your business, your stakeholders and your regulators.

Our data protection professionals are commercially minded and risk focused. They bring together a range of specialisms to advise on best practice and offer assurance on all aspects of data protection, breach management and cyber resilience.

We can support you by:

- carrying out a gap analysis to identify key processes and risks to personal data
- recommending an appropriate risk and control framework
- drafting appropriate policies and procedures to support the new requirements
- delivering GDPR audits
- reviewing your data protection compliance programmes
- supporting those responsible for data protection and helping to embed the necessary skillsets within your organisation.

Grant Thornton Limited is the Channel Islands member firm of Grant Thornton, one of the world's leading international organisations of independently owned and managed accounting and consulting firms. We can draw on this global network and wealth of multidisciplinary experience to offer value adding advice, tailored to your needs. Grant Thornton has member firms across 130 countries to support your international privacy obligations.

For further information, please contact:

David Cartwright
Senior Consultant
Information Security
T +44 (0)1534 885813
E david.cartwright@gt-ci.com

Grant Thornton
An instinct for growth™

grantthorntonci.com

GRT106223