EU General Data Protection Regulation

A Compliance Guide

December 2016

Protect • Comply • Thrive

Getting ready for GDPR compliance

The introduction of the European General Data Protection Regulation (GDPR) heralds the most significant change to data protection law in the EU, and globally, in recent years. In this green paper, we give an overview of the key changes presented by the Regulation, and the critical areas to be aware of when preparing for compliance.

Introduction

The EU General Data Protection Regulation (GDPR) was adopted in April 2016 and will take effect across the European Union (EU) on 25 May 2018, when it supersedes the 28 current national data protection laws based on the 1995 Data Protection Directive (DPD).

Introduced to keep pace with the modern digital landscape, the purpose of the new Regulation is twofold:

1. to improve consumer confidence in organisations that hold and process their personal data by reinforcing their privacy and security rights consistently across the EU, and
2. to simplify the free flow of personal data in the EU through a coherent and consistent data protection framework across the member states.

The new Regulation does not fundamentally change any of the core rules in the DPD; it instead extends the Directive's requirements significantly by introducing a range of new obligations to support those core rules. These additional obligations will be familiar in some member states. For example, Germany already imposes an obligation to appoint data protection officers, has the concept of pseudonymised data and has extensive requirements for processors' contracts. In other member states, these obligations will be very new.

A matter of urgency

Every organisation that processes or shares personal data now has less than 18 months to comply with the new Regulation. This involves organisations understanding what personal data they currently hold or process and the risks to that data, adapting their business processes and infrastructure, implementing tools and compliance processes, and changing the way they collaborate with suppliers. In some instances, those changes could be significant and work will need to start as a matter of urgency. Bear in mind that every organisation in the EU is simultaneously faced with the same timetable, and that skilled compliance resources are already in short supply.

Regulatory compliance may be viewed by many as an administrative burden. However, ignoring the GDPR or getting it wrong could have costly repercussions: organisations found to be in breach of the Regulation face **administrative fines of up to 4% of their annual global turnover or €20 million** – whichever is greater.

Organisations that take the time to properly prepare for and comply with the new Regulation will not only avoid significant fines and reputational damage, but will also find that their data handling, information security, compliance processes and contractual relationships are more robust and reliable.

Key changes:

GLOSSARY

Data controller (organisation) means "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".

Data subject (individual) means an identifiable natural person "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier.

Personal data means "any information relating to an identified or identifiable natural person ('data subject')". The Regulation states this also includes online identifiers such as IP addresses and cookies.

Data processor (service providers) means "a person, public authority, agency or other body which processes personal data on behalf of the controller". An example is a Cloud provider that offers data storage.

1. Scope of the new law

Harmonisation – only one law

There are currently 28 different sets of data protection laws across the European Union. The GDPR will replace these with a pan-European regulatory framework effective from 25 May 2018. As a Regulation, it is directly effective in all member states without the need for further national legislation.

For organisations that operate across multiple member states, this harmonisation is welcome. However, some national divergences are likely to remain and further divergences may arise because member states have limited rights to amend some of the obligations under the Regulation:

- Employment – member states can introduce further restrictions on the processing of employee data.
- National security – member states can pass laws to limit rights under the Regulation in areas such as national security, crime and judicial proceedings.

Although the Regulation has been published, there is still uncertainty about what some of the provisions mean or how they should be applied. Different social and cultural attitudes to data protection will influence their interpretation, and what is regarded as "high risk" in Berlin may not also be regarded as "high risk" in Rome.

Finally, differences in the resources and attitudes of supervisory authorities may result in wide variations in enforcement. There is a wide discrepancy between the theoretical powers open to national regulatory authorities and the application of those powers in practice.

Issues of this sort will be resolved in the normal course of regulatory business. Organisations still face the 25 May 2018 compliance deadline.

Expanded territorial reach

The GDPR applies to all EU organisations – whether commercial business or public authority – that collect, store or process the personal data of EU individuals.

Organisations based outside the EU that monitor or offer goods and services to individuals in the EU will have to observe the new European rules and adhere to the same level of protection of personal data.

The Regulation also requires such organisations – controllers and processors – to appoint an EU representative based in one of the member states in which the relevant individuals are based. This is unless the processing is occasional and does not include large-scale processing of special categories of data or processing of data relating to criminal convictions and offences.

Single scheme "one-stop shop"

A new one-stop shop provision means that organisations will only have to deal with a single supervisory authority, not one for each of the EU's 28 member states, making it simpler and cheaper for companies to do

business in the EU. An organisation that carries out cross-border processing should be primarily regulated by the supervisory authority in which it has its main establishment (the lead supervisory authority).

Obligations on processors

The Regulation also introduces obligations on data processors. These are service providers that process personal data on behalf of organisations but do not determine the purpose or means of the processing, such as call centres.

Where a controller contracts a processor to process personal data, that processor must be able to provide "sufficient guarantees to implement appropriate technical and organisational measures" to ensure that processing will comply with the GDPR and that data subjects' rights are protected. This requirement flows down the supply chain, so a processor cannot subcontract work to a second processor without the controller's explicit authorisation.

Contractual arrangements will need to be updated, and stipulating responsibilities and liabilities between the controller and processor will be imperative in future agreements. Parties will need to document their data responsibilities even more clearly and the increased risk levels may impact service costs.

2. Individuals' data rights

Core rules remain the same

Many of the core definitions from the DPD remain largely unchanged. In particular, the Regulation retains the very broad definition of personal data and processing, and organisations must comply with all six general principles when processing personal data. Some important new concepts are "high risk to individuals", "large scale processing" and "pseudonymised data" (data from which no individuals can be identified without the use of additional information).

Consent

The Regulation imposes stricter requirements on obtaining valid consent from individuals to justify the processing of their personal data. Consent must be a "freely given, specific, informed and unambiguous indication of the individual's wishes". Silence, pre-ticked boxes or inactivity do not count as consent. The organisation must also keep records so it can demonstrate that consent has been given by the relevant individual. Finally, consent must be explicit when processing sensitive personal data, or transferring personal data outside the EU.

Additional protection for children

Consent from a child in relation to online services is, under the new Regulation, only valid if authorised by a parent. A child is someone below the age of 16, though member states can reduce this age to 13.

New data access rights

One of the key aims of the Regulation is to empower individuals and give them control over their personal data. While the Regulation largely preserves the existing rights of individuals to access their own personal data, require rectification of inaccurate data, object to direct marketing, and challenge automated decisions about them, it also confers significant additional new rights for individuals.

- **Right to be forgotten**
  Individuals have a new right to require the data controller to erase all personal data held about them in certain circumstances, such as where the data is no longer necessary for the purposes for which it was collected. There are a number of exemptions to this right, for example in relation to freedom of expression and compliance with legal obligations. It is likely that the limits of this right will be fought over in EU law courts for many years.
- **Right to data portability**
  This is a new concept under the Regulation. Individuals will have the right to transfer personal data from one data controller to another where

processing is based on consent or necessity for the performance of a contract, or where processing is carried out by automated means.

Profiling

Data controllers must inform data subjects of the existence and consequences of any profiling activities that they carry out (including online tracking and behavioural advertising).

Organisations that collect and use personal data will need to put in place more robust privacy notices than have previously been required, providing more information in a more prescribed manner. This will involve a large-scale review of all privacy notices.

3. Data protection

Data protection by design

The Regulation cannot be satisfied with 'tick-box' compliance; compliance must become part of 'business as usual'. The key to accountability is to embed compliance into the fabric of your organisation. This includes not just developing appropriate polices but also applying the principles of **data protection by design and by default.**

Specifically, organisations must take appropriate technical and organisational measures before data processing begins to ensure that it meets the requirements of the Regulation. Data privacy risks must be properly assessed, and controllers may use adherence to approved codes of conduct or management system certifications, such as ISO 27001, to demonstrate their compliance.

Data protection impact assessment (DPIA)

Data protection must now be designed into processing systems by default and a DPIA is now mandatory in certain circumstances. Good practice for new technologies and processes is to assess whether processing has a "high risk" of prejudicing data subjects' rights, and whether this risk can be reduced or avoided, for example by pseudonymisation. A DPIA shall "in particular" be required where there is automatic processing (including filing) and processing of special categories of data on a large scale.

Compliance standards

The GDPR encourages the adoption of certification schemes as a means to demonstrate compliance. Compliance with the international information security standard ISO 27001 – the only independent, internationally recognised data security standard – will help organisations demonstrate that they have endeavoured to comply with the data security requirements of the GDPR. Implementing ISO 27001 involves building a holistic framework of processes, people and technologies in order to secure information.

Records of data processing

The Regulation now places the onus on organisations and data processors to keep their own records of data processing activities and make these available to the supervisory authority on request. This record needs to contain a specific set of information so that it is clear what, where, how and why data is processed. Small businesses employing fewer than 250 employees are exempt from these record-keeping requirements unless their processing activities involve a risk to the rights and freedoms of data subjects, are not occasional, or include special categories of personal data or data relating to criminal convictions or offences.

4. Accountability

Data protection officer

Many organisations will be required to appoint a data protection officer (DPO) to be responsible for monitoring compliance with the Regulation, providing information and advice, and liaising with the supervisory authority. They are an existing feature of some member states' data protection laws, such as Germany.

A DPO must be appointed where:

- the processing is carried out by a public authority;
- the organisation's core activities require regular and systematic monitoring of data subjects on a large scale; or
- the organisation's core activities consist of the large-scale processing of special categories of data and data relating to criminal convictions and offences.

In most organisations, it will be good practice to appoint a DPO anyway. The GDPR obligations are such that having readily available advice and support from a data protection specialist will be an essential risk management step, in the same way that organisations now appoint HR or health and safety managers.

The DPO, where appointed, must be independent. This does not mean you have to appoint an external person; the DPO role can be fulfilled by an employee. The post can be a part-time role or combined with other duties, but, in performing the role, the DPO must have an independent reporting line and be empowered to report directly to the board without interference. What is important is that the appointed person must be a data protection professional with "expert knowledge of data protection law and practices" to perform their duties.

- **What qualification does the data protection officer need?**

  The data protection officer must have the right professional qualities and knowledge of data protection law. There is currently no express requirement to hold any particular qualification or certification. However, obtaining training and qualifications in GDPR compliance would be an effective way to demonstrate expert knowledge. The IBITGQ ISO 17024-accredited EU GDPR Practitioner (EU GDPR P) is one such qualification.

Data breach notification and penalties

The increase in high-profile cyber attacks is reflected in the enhanced data security obligations in the Regulation and the parallel obligations in the **Network and Information Security Directive.**

It will be mandatory for an organisation to report any data breach to its supervisory authority within 72 hours of becoming aware of it. If that requirement is not met, the eventual report must be accompanied by an explanation for the delay. The notification must include specific information, including a description of the measures being taken to address the breach and mitigate its possible side effects.

Where the breach may result in a high risk to the rights and freedoms of individuals, the individuals themselves must be contacted "without undue delay". This contact will not be necessary if appropriate protective measures – essentially encryption – are in place to eliminate danger to data subjects.

Any infringements of the new Regulation are subject to a tiered financial penalty regime with **fines of up to 4% of annual global turnover or €20 million, whichever is the greater**. In determining the level of the fine, the supervisory authority must consider a range of factors including the gravity of the breach, whether the breach was intentional or the result of negligence, and any steps taken to mitigate the breach. Additionally, individuals can sue organisations for compensation to cover both material and non-material damage (e.g. distress).

Given the magnitude of potential fines, the rights of individuals to bring cases and claim compensation, and the prevalence and effectiveness of cyber crime, the risk of a data breach should go straight onto the board's risk register, with compliance high on senior management's agenda.

5. Data transfers outside the EU

The Regulation prohibits the transfer of personal data outside the EU to a third country that does not have adequate data protection. The European Commission has the power to approve particular countries as providing an adequate level of data protection, taking into consideration the data protection laws in force in that country and its international commitments. At present this list is Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

For data transfers to any country not on the list, there must be a legal contract that stipulates that the non-EU recipient agrees to the data protection safeguards required. The Regulation explicitly recognises and promotes the use of binding corporate rules as a valid data transfer mechanism within groups of companies. Approved codes of conduct also can be used for data transfers.

Preparing for GDPR compliance

There are clearly a number of key critical areas to observe in your approach to ensure GDPR compliance. Plenty of obligations can be resolved fairly simply and quickly. Others, particularly in large or complex organisations, could have significant budgetary, IT, personnel, governance and communications implications. Ensuring buy-in from senior management and key stakeholders in your organisation will be critical to meeting your obligations.

An important next step will, for most organisations, be to gain clarity on their personal data processing, and includes identifying:

- What personal data is held across the organisation
- What permissions have been obtained for that data
- What processes and systems are in place for handling personal data
- Where personal data is transferred outside the organisation (including third parties and cross-border)
- How personal data is secured throughout its lifecycle

With an understanding of the compliance gaps, organisations will be in a position to assess their personal data risks and develop an appropriate remediation plan.

The time to start planning for GDPR compliance is now.

How we can help

A leading global authority on data protection, IT Governance helps organisations address the challenges of GDPR compliance with a comprehensive suite of information resources, solutions and advisory services.

GDPR compliance solutions and services			
Information resources	**GDPR bookshop**		
	EU GDPR – A Pocket Guide	EU GDPR – An Implementation and Compliance Guide	
Education	**GDPR training courses**		
	• Certified EU General Data Protection Regulation Foundation • Certified EU General Data Protection Regulation Practitioner		
	Classroom	Live Online	Distance learning
Compliance tools	**GDPR toolkits**		
	EU GDPR Documentation Toolkit		
Advice and consultancy	**GDPR transition services**		
	Data Flow Audit	GDPR Gap Analysis	GDPR Transition
Certification	**Information security management system**		
	ISO 27001 certification		

About the author

Alan Calder is an acknowledged international cyber security guru and a leading author on information security and IT governance issues. He is also chief executive of IT Governance Limited, the single-source provider for products and services in the IT governance, risk management and compliance sector.

Alan wrote the definitive compliance guide, *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002* (co-written with Steve Watkins), which is the basis for the UK Open University's postgraduate course on information security. This work draws on his experience of leading the world's first successful implementation of BS 7799 (now ISO 27001).

Alan is a frequent media commentator on information security and IT governance issues, and has contributed articles and expert comment to a wide range of trade, national and online news outlets.

GDPR compliance products and services

Books

- **EU GDPR: A Pocket Guide**
  The perfect introduction to the principles of data privacy and the GDPR, this concise guide is essential reading for anyone wanting an overview on the new compliance obligations for handling the personal data of EU residents. The guide is also available in French, German, Italian and Spanish.
  Click for further information and to purchase the book >>

- **EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide**
  This clear and comprehensive guide provides detailed commentary on the GDPR and practical implementation advice on the compliancy measures needed for your data protection and information security regimes.
  Click for further information and to purchase the book >>

Training courses

- **Certified EU GDPR Foundation training course**

  This one-day course will offer a solid introduction to the European General Data Protection Regulation and provide a practical understanding of the implications and legal requirements of the Regulation, culminating in an official certification from the International Board of IT Governance Qualifications (IBITGQ).

  Click for further information and to book a course >>

- **Certified EU GDPR Practitioner training course**

  This comprehensive training course prepares individuals who are seeking to embed their knowledge of the EU GDPR in order to serve as their organisation's data protection officer (DPO). The course will cover aspects of the Regulation in depth, including implementation requirements, the necessary policies and processes, as well as recognised data security risk analysis methods.

  Click for further information and to book a course >>

Documentation toolkits

- **EU GDPR Documentation Toolkit**

  A full set of policies and procedures enabling your organisation to comply with the EU GDPR. These digital templates are fully customisable and significantly reduce the burden of developing the necessary documents to achieve legal compliance.

  Click for further information and to download a free trial version >>

Advice and consultancy

- **GDPR data flow audit**

  For this essential first step in the preparation process, our privacy experts provide a data inventory and flow map of the personal data held and shared by your organisation. This forms the basis for assessing the information privacy and security risks in your organisation.

  GDPR Gap Analysis

  Delivering a targeted assessment of your compliance with the GDPR, our privacy experts provide a detailed assessment of your readiness, key gaps and risks, and a remediation roadmap.

  Click for further information and to contact IT Governance for assistance >>

Certification

- **Information security management system: ISO 27001**

  Internationally recognised as an effective way to demonstrate that "appropriate technical and organisational measures have been implemented" to meet GDPR requirements, our leading ISO 27001 implementation specialists will help your organisation achieve certification.

  Contact IT Governance for assistance at servicecentre@itgovernance.eu >>

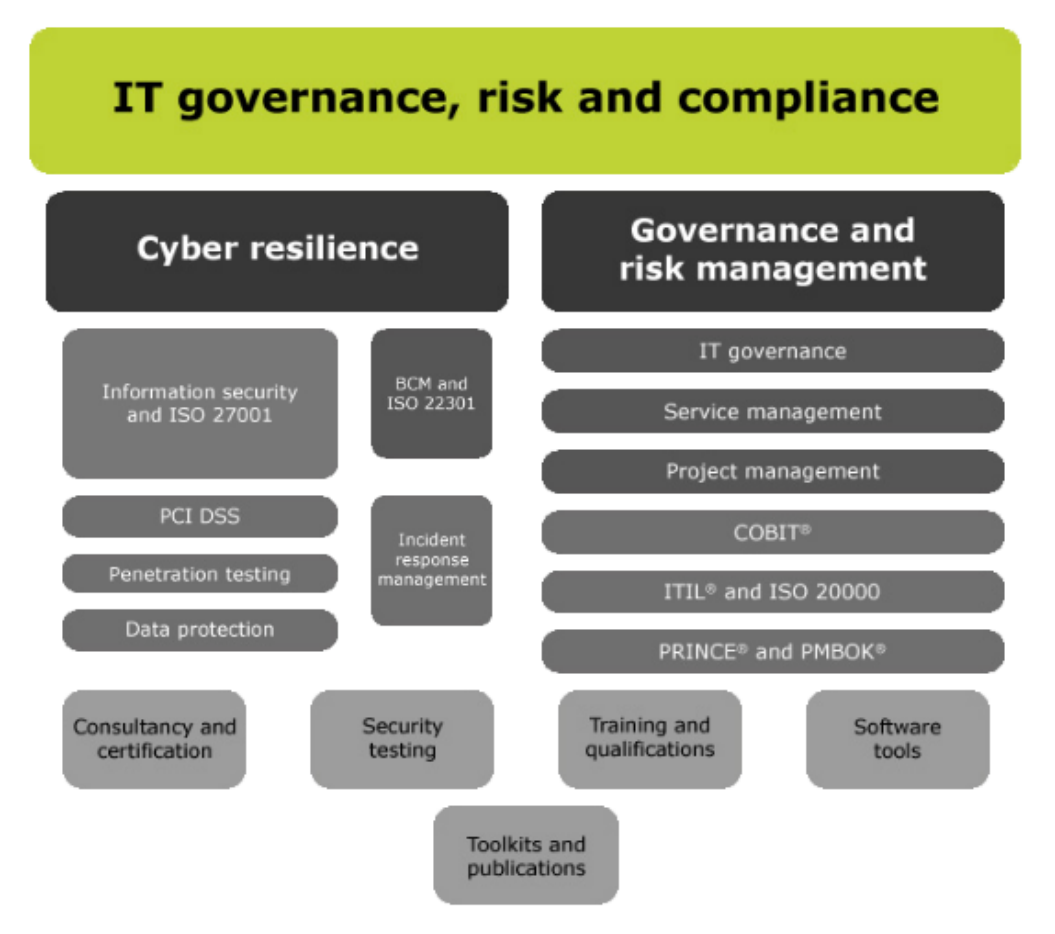
IT Governance Solutions

IT Governance sources, creates and delivers products and services to meet the evolving IT governance needs of today's organisations, directors, managers and practitioners.

IT Governance is your one-stop shop for corporate and IT governance information, books, tools, training and consultancy. Our products and services are unique in that all elements are designed to work harmoniously together so you can either benefit from them individually or combine different elements to build something bigger and better.

Our **Protect - Comply - Thrive** approach is aimed at helping your organisation achieve resilience in the face of constant change.

Our areas of expertise:



Contact us:
www.itgovernance.eu
+ 44 (0)845 070 1750
servicecentre@itgovernance.eu