ReedSmith

The business of relationships.

IP, Information and Innovation

Data Protection

GDPR: Preparing for the European General Data Protection Regulation

Contents

The Background: from Directive to Regulation

For a little over 20 years, the protection of individuals in relation to the collection, use and processing of their personal data has been governed in Europe by the Data Protection Directive (95/46/EC) (the Data Protection Directive), adopted and implemented in national law by all 28 EU member states.

Reform began in 2012 aimed at harmonising data protection across the EU via a General Data Protection Regulation, which, as an EU regulation, would have direct effect across all EU member states. This reform also sought to ensure that the governing law was updated to account for the rise of personal technology and the vast array of devices now at the EU's disposal. New technology means new risks as well as new ways of collecting and using data.

It took nearly four years of consultation to agree the General Data Protection Regulation (the GDPR or Regulation) and it was formally adopted on 27 April 2016 and published in the *Official Journal of the European Union* on 4 May 2016, entering into force 20 days later. A transitional period of two years was then agreed, during which organisations would have time to prepare for 25 May 2018, when the Regulation becomes enforceable.

The long arm of the law

The GDPR applies to controllers and processors "regardless of whether the processing takes place in the European Union or not". The extra-territorial application of the GDPR is triggered when:

- goods or services are offered to EU citizens; or
- the behaviour of EU citizens is monitored or tracked through the use of technology.

Organisations which do not have an establishment in the EU – and which consider themselves to operate outside the scope of EU data protection law – are now subject to data protection regulation pursuant to the GDPR.

How does this affect your business?

By the time the GDPR is applied in May 2018, you will need to make sure that all practices, policies and processes relating to the collection and use of personal data across your organisation have been assessed and brought into alignment with the requirements of the new Regulation.

We have prepared this publication to lay out the new obligations being ushered in by the GDPR, in order for you to better understand what the Regulation expects from your business in relation to the data you hold, whether it relates to your employees, customers or suppliers.

Data Protection Principles

Article 5 of the GDPR sets out the major principles that all organisations are required to comply with when they process personal data.

Lawfulness, fairness and transparency	Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes
Data minimisation	Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data must be accurate, and where necessary, be kept up to date
Storage limitation	Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data must be processed in a way that ensures appropriate security of personal data
Accountability	The controller shall be responsible for, and be able to demonstrate, compliance with the principles

Accountability and Governance

Some of the most important new requirements under the GDPR are those pertaining to accountability. Accountability means that organisations must demonstrate compliance with the GDPR.

What will Accountability actually look like under the Regulation?

Under the GDPR, there is no change in the definitions of the two key roles of data controller and data processor but how liabilities are negotiated—we expect increased complexity (at least initially)—to change. Why?

Simply stated, for the first time data processors will take on a direct regulatory responsibility and, therefore, liability. Supervisory authorities may develop a new 'contributory negligence' approach to enforcement and sanctions.

Controller

A data controller can be an individual or an entity. Data controllers determine the purposes for and means of processing personal data, and are accountable for compliance with the GDPR principles.

Processor

A data processor is an individual or entity which processes personal data on behalf of a controller.

The concept of the data processor is well known from the Data Protection Directive. For the first time, data processors are subject to direct regulation by supervisory authorities under the GDPR. Although processors have several obligations, two of the most notable are:

- Implementation of sufficient security measures, having regard to the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing.
- Maintenance of records of all categories of processing activities carried out on behalf of a data controller, including details of any international data transfers.

Accountability in practice

Data controllers will continue to be responsible and accountable for compliance and governance, with the GDPR elevating the significance of their role.

Data processors will be in line for greater liability now that they will be directly regulated. As a result, we expect to see a significant impact on contracts with service providers.

Data Protection Officers (DPOs) will assume a vital and powerful role. We may see increasingly the voluntary appointment of DPOs as a means of centralising the accountability function.

Governance

Accountability means that governance structures must have the spotlight shone on them. With the requirement for some organisations to appoint a DPO – as a minimum governance

requirement – some aspects of governance may become more prescriptive, with some decisions taken out of the hands of business.

In practice, organisations will be expected to put into place comprehensive but proportionate governance measures, including:

- Appropriate technical and organisational measures
- Recording of processing activities
- Appointment of a Data Protection Officer (where appropriate)
- Implementation of Data Protection by Design and by Default
- Development and use of Data Protection Impact Assessments

Demonstrating Compliance

As part of accountability, organisations must be able to demonstrate not only that they have a compliance framework in place but also that they implement and adhere to these measures.

Rights of Individuals

The GDPR preserves a number of existing rights of data subjects to access their personal data but importantly, as well as providing further obligations on those existing rights, it also creates new rights. The below table summarises the impact and key obligations as regards controllers receiving requests from data subjects.

Right	Requirement
	New Rights
Right to restrict processing	Controller to cease processing where: (i) accuracy is contested by the data subject; (ii) processing is unlawful but the data subject does not request erasure; (iii) processing is no longer necessary; or (iv) data subject has objected to the processing and controller determines that no overriding legitimate grounds exist. If data disclosed to third party, controller to inform them of restriction unless this is impossible or involves disproportionate effort.
Rights against automated decision making and profiling	Controller to identify whether operations constitute automated decision making and update such operations so as to ensure process allows for human intervention. Exemptions available to controller.
Right to data portability	Controller to provide the personal data (that are processed in an automated way) in a structured, commonly used and machine-readable format and, where requested and technically feasible, transmit them directly to another controller.

Right	Requirement	Changes to existing law(s)
	Existing Rights	
Right to be informed	Controller to provide data subjects with information relating to the processing of their personal data in a concise, clear and intelligible manner.	More detailed information to be provided and depends on whether data obtained directly from data subject.
Right of access	Controllers to confirm whether personal data are being processed, and if so, provide access.	Information to be provided free of charge and within one month of receipt. Where request made electronically, information to be provided in a "commonly used electronic format".
Right to rectification	Controller to rectify inaccurate or incomplete personal data without undue delay.	Where controller has disclosed personal data to third party, controller to inform them of rectification.
Right to object	Controller to cease processing where data subject objection to processing is: (i) based on certain grounds (public interest or legitimate interest); or (ii) for certain purposes (research or statistics). Some exemptions may be available to controller. Data subject has absolute right to object to data processed for direct marketing purposes. No exemptions are available to controller.	Right to object to personal data being used for statistical or research purposes.
Right to erasure ('right to be forgotten')	Controller to erase personal data when: (i) no longer necessary; (ii) consent is withdrawn; (iii) data subject objects and controller has no overriding legitimate grounds to hold data; (iv) data is unlawfully processed; (v) necessary to comply with a legal obligation; or (vi) processed in connection with an online service offered to a child.	Broader, more specific rights created. If data disclosed to third party, controller must inform them of erasure unless it is impossible or involves disproportionate effort.

Embedding Data Protection in Your Organisation

Data Protection Impact Assessment (DPIA) is a process involving the identification, assessment and minimisation of data protection risks

Data Protection Impact Assessments

DPIAs are mandatory when processing poses a "high risk" to the rights and freedoms of individuals. Examples of **"high risk" operations** include:

- New technologies
- Profiling or automated processing
- Processing sensitive data (special categories of data) on a large scale
- Systematic monitoring of public areas (e.g., CCTV/video surveillance)

Once the need for a DPIA has been identified, a number of steps must be taken:

- **Description of processing operations envisaged and purposes of processing**
  - Describe how personal data is: (i) collected, (ii) used, and (iii) deleted
  - What legitimate interest is the controller pursuing?
- **Assessment of necessity and proportionality of processing operations**
  - How many individuals are likely to be affected?
- **Identification and assessment of data protection risks**
  - What steps are taken to address risk to: (i) the individual, and (ii) the organisation?
- **Identification and evaluation of data protection solutions**
  - Evaluate proposed measures and safeguards for addressing risk
  - What level of risk is acceptable?
- **Approval and recording**
  - Ensure DPIA receives sign-off at the appropriate level
  - Record decisions taken to eliminate, mitigate or accept risk, and demonstrate compliance
- **Integration of DPIA outcomes in the project plan**
  - Implement, monitor, re-assess and update the DPIA plan over the life-cycle of the project and when there is a change of risk

Prior consultation with lead Data Protection Authority

In the absence of measures to mitigate risk where high risk is identified, the controller **must consult the supervisory authority prior to processing**.

Worth considering...

- Organisations should think about putting a standard template in place for their business to use for any new process or activity that involves the processing of data.

Data Protection: by Design or by Default?

Data Protection is set to become an integral part of both the technological development and organisational structure of new products or services.

The GDPR introduces Data Protection by Design and Data Protection by Default, which, in practice, means that all organisations must take data protection into consideration from the outset of projects or new initiatives.

Data Protection by Design

An organisation needs to show that adequate security measures have been implemented and that compliance is monitored. Data protection is baked in, not bolted on from at the concept phase of any product or service or use of technology.

Appropriate technical and organisational measures become part of the development for each new project, service or business process.

It must be demonstrated that sufficient account is taken in regard to:

- **Nature, scope, context** and **purposes of processing**
- **Likelihood** and **severity of risks** to rights and freedoms of individuals

Data Protection by Default

Data Protection by Default means that the strictest privacy settings automatically apply once a customer acquires a new product or service.

By default only personal data which are necessary for specific identified purposes are processed.

This applies to:

- **Amount** of personal data collection
- **Extent** of processing
- **Period of time** for storage of personal data
- **Accessibility**

At what stage of the project?

- At the time when determination of the means of processing is made
- At the concept and design phase of any project

From the outset

- Organisations must take data protection into consideration from the outset of any new project, making it an integral part of the project development process... **from day one**.

Supply Chain

The greatest impact of the GDPR on a controller's dealings with its suppliers amounts to ensuring sufficient guarantees of data protection. This was previously being seen in the Data Protection Directive but was not anchored as a legal requirement in such explicit terms as we see now. However, as with several aspects of the GDPR, greater clarity is expected through regulatory guidance as well as EU member states' delegated powers.

Supplier due diligence

Controllers are required to carry out due diligence on suppliers (processors) processing personal data on their behalf. They will need to ensure suppliers can provide sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of the Regulation, including measures to ensure the security of processing.

Supplier obligations

The processing by a supplier should be governed by a written, binding contract, setting out the subject matter, duration, nature and purposes of the processing, the type of personal data and the data subjects. It must also take into account the specific tasks and responsibilities of the supplier and the risks involved to the rights and freedoms of the data subjects. Under article 28 of the GDPR the contract must stipulate that the supplier:

- only processes personal data on documented instructions;
- ensure those with access to personal data have committed themselves to confidentiality;
- takes all security measures required under the Regulation;
- ensures the same obligations flow down to sub-contractors;
- assists the controller with regards compliance with their obligations under the Regulation, including responses to requests by individuals to exercise their rights under the Regulation;
- deletes or returns all personal data at the end of the arrangement; and
- makes available all information necessary to demonstrate compliance with their obligations.

How does this affect your business?

All contracts involving personal data handling or transfers must comply with the GDPR as at 25 May 2018 – in other words, we are currently in the transition period.

Organisations should review their existing arrangements with service providers, starting with the most critical services for their business operations. Start negotiations well in advance of the GDPR deadline – otherwise you will risk being non-compliant or having third party standard terms imposed on you which could be (a) non-compliant from your perspective and/or (b) unfavourable.

International Data Transfers

Under the GDPR, data transfers to countries outside of the European Economic Area (EEA) remain subject to restrictions. Restrictions also apply to "onward transfers" of data from an importer to another third country or organisation.

International transfers under the GDPR can take place on the following bases:

1 Adequacy Decisions

If the European Commission has adopted a decision that the third country, territory or sector involved in the transfer provides an 'adequate' level of protection for the data being transferred, data may flow freely between the EEA and country, territory or sector.

2 Appropriate Safeguards

- **Model clauses**

  Model contractual clauses approved by the European Commission may be used in order to legitimise transfers between the contracting parties.

- **Binding Corporate Rules**

  Binding Corporate Rules ("BCRs") are explicitly recognised in the text of the GDPR, which infers a level of legitimacy. BCRs are a method of legalising the international transfer of personal data within a group of companies and are available for both controllers and processors.

- **EU Codes of Conduct**

  The GDPR provides that approved codes of conduct along with binding and enforceable commitments of the controller or processor may be used. No such codes of conduct have yet been approved.

- **EU Certification**

  The GDPR also provides for approved certification mechanisms to be used as a basis for data transfers along with binding enforceable commitments with the controller or processor. No such certification mechanisms have yet been approved.

3 Specific Derogations

- **Explicit consent**
- **Contract performance**
- **Public interest**
- **Legal claims**
- **Vital interests**
- **Public source**

Worth noting...

- In exceptional cases, the controller may also invoke his compelling legitimate interest as a new specific derogation.

Data Protection Officers

Whilst some organisations can volunarily appoint a data protection officer (DPO) as part of their accountability programme, in certain circumstances the appointment of a DPO is mandatory.

Controllers and processors must appoint a DPO where:

- the processing is carried out by a **public authority**;
- **the core activities** of the controller or processor consist of processing which, by its nature, scope or purposes, requires **regular and systematic monitoring of data subjects on a large scale**; or
- the core activities consist of processing on a **large scale of special categories of data**.

The DPO can be an employee of the organisation or hired externally, and companies within a corporate group can appoint a single DPO.

The DPO must be designated on the basis of professional qualities, in particular their expert data protection knowledge and ability to fulfil their DPO responsibilities.

DPO responsibilities

The DPO will be responsible for informing and advising on the organisation's data protection obligations, advising on the performance of data protection impact assessments, and cooperating with the supervisory authority.

The DPO must **monitor compliance** with the GDPR, with other EU or national data protection laws, and with their organisation's policies on the protection of personal data. This includes **assigning responsibilities, raising awareness** and **staff training**.

Position of the DPO

Organisations must ensure that the DPO can operate independently of instruction, cannot be dismissed or penalised for carrying out their responsibilities and is to **report directly to the highest level of management.**

Case Study...

LiveWell, Inc. is a U.S. headquartered business offering health and wellness products and services across the globe, including to 650,000 customers in the EU. LiveWell regularly carries out customer surveys and trials for research and product development purposes. Data are hosted by Cirrus Limited, a cloud provider in Ireland, though certain business functions in the United States have access to data for management and IT operations. **Will LiveWell need to appoint a DPO?**

As yet there is no regulatory guidance, but the potential volume of data, including sensitive personal data, processed by LiveWell could make it subject to the DPO requirement.

Data Breach Notifications

The GDPR will require data breach notification to an organisation's lead data protection authority and, in certain circumstances, to affected individuals.

New rules

In the event of a data breach, controllers will be required to notify:

- The national supervisory authority where the breach would likely result in the risk to the rights and freedoms of individuals.
- Individuals affected where the breach would likely result in a high risk to their rights and freedoms.

Notice to the Supervisory Authority

Notification to the relevant supervisory authority must be within 72 hours of becoming aware of the breach. Failure to notify when required to do so could result in a fine of up to €10 million or 2 per cent of global turnover.

When you notify you should include:

- the nature of the breach, including categories of individuals and the approximate number of records involved;
- the details of the DPO or another person if there is no DPO;
- the likely consequences of the breach; and
- a description of any, or proposed, remedial action taken.

Notices to Affected Individuals

High risk data breaches must be notified to affected individuals without undue delay, unless an exemption applies, and must contain the following information in clear and plain language:

- the nature of the breach;
- the likely consequences of the breach; and
- a description of remedial action taken as well as information about any actions the individual should take to minimise possible adverse effects.

How to prepare

- **Training and awareness:** ensure everyone in your organisation who handles personal data is aware of what amounts to a breach.
- **Response plan**: have an internal breach response plan that provides for robust breach detection methods, investigations and an internal reporting procedure.

Supervisory Authorities and Sanctions

Supervisory authorities will continue to play a vital role under the GDPR. Each member state must have established at least one independent supervisory authority which will be responsible for enforcing the GDPR.

Controllers and processors must have a "lead supervisory authority" located in the jurisdiction where they have their main or sole establishment. There are complex rules in place to govern cooperation between an entity's lead supervisory authority and other supervisory authorities, which take effect where a complaint is made by a data subject. There are also mutual assistance provisions in place, and supervisory authorities may operate jointly to conduct investigations and take enforcement action.

A European Data Protection Board, tasked with ensuring the consistent application of the GDPR, will also be established. The Board will have a number of responsibilities, including issuing guidance on a number of topics and resolving disputes between supervisory authorities.

Powers of Supervisory Authorities

Supervisory authorities have robust enforcement powers which go far beyond those under the Data Protection Directive. Supervisory authorities may, for example:

- order controllers or processors to provide information
- access a controller or processor's premises and equipment
- issue warnings and reprimands;
- limit or ban data processing
- impose administrative fines of up to €20,000,000 or 4 per cent of total worldwide turnover.

The scope of enforcement powers available to supervisory authorities and their implications for businesses will ensure that GDPR compliance remains a board-level concern.

Putting the Theory into Practice: What Next?

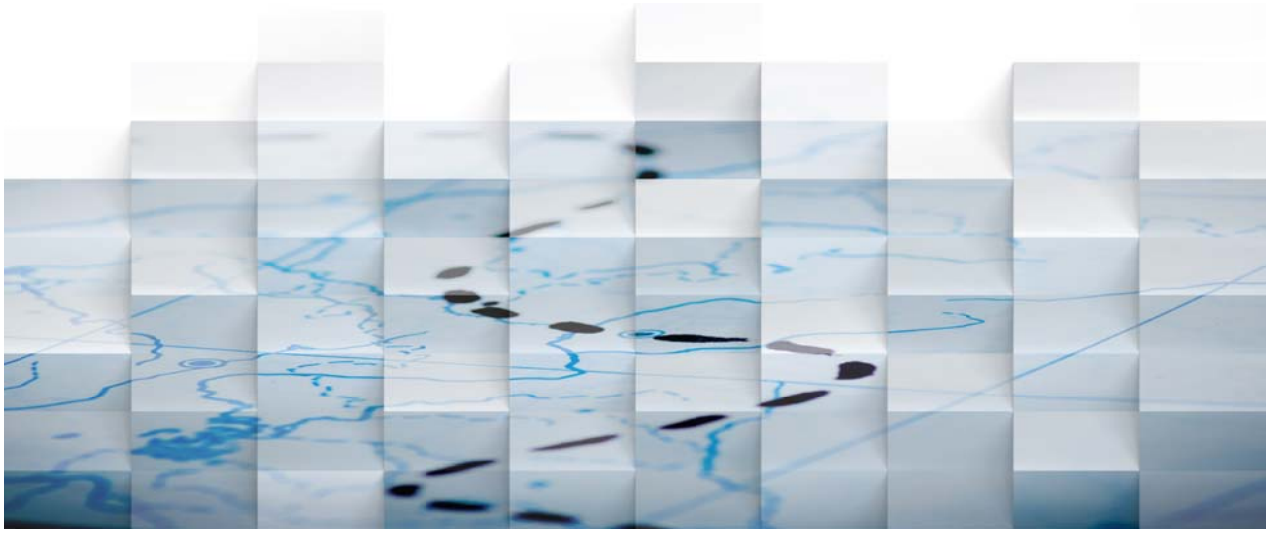
In a nutshell:

The GDPR will be fully in force from 25 May 2018 and will apply in the UK and across all EU member states. The countdown has already begun so your organisation must have everything prepared and in place for this seismic shift in the regulatory landscape.

Path to compliance

The ten steps to compliance are:

1. **Stakeholder Awareness:** Embed data protection in your organisation
2. **Data Inventory:** Assess and record the personal data being processed
3. **GDPR Gap Analysis:** Determine what additional steps are required for GDPR compliance
4. **Implementation Plan:** Create a project plan to address the compliance gaps
5. **Governance Structure & DPO:** Appoint data protection officer and create governance structure to support accountability requirements
6. **Supply Chain (Processors):** Ensure supplier contracts are amended to meet GDPR requirements
7. **Cross-Border Transfers:** Review cross-border data transfers
8. **Accountability Processes:** Utilise tools and processes to document compliance
9. **Data Subjects' Rights:** Put in place policies and procedures to ensure rights are respected
10. **Data Breach Notification:** Create policy for breach response, containment, remediation and notifications



Our European Team

As part of the IP, Information and Innovation Group, our IT, Privacy and Data Security team brings strength and increased connectivity in today's information economy by developing a collaborative, cross-discipline practice focusing on data security, information governance, technology, and intellectual property services. We have included below details of our key European contacts. Our global team consists of over 60 lawyers across our offices in Europe, the United States, Asia and the Middle East.

London

Cynthia O'Donoghue
Partner, International Head of IT, Privacy & Data Security
London
+44 (0)203 116 3494
codonoghue@reedsmith.com

Philip Thomas
Counsel
London
+44 (0)203 116 3526
pthomas@reedsmith.com

Katalina Bateman
Senior Associate
London
+44 (0)203 116 2866
kbateman@reedsmith.com

Chantelle Taylor
Associate
London
+44 (0)203 116 3481
ctaylor@reedsmith.com

Curtis McCluskey
Associate
London
+44 (0)203 116 3467
cmccluskey@reedsmith.com

Tom Evans
Associate
London
+44 (0)203 116 3653
tevans@reedsmith.com

Paris

Daniel Kadar
Partner
Paris
+33 (0)1 76 70 40 86
dkadar@reedsmith.com

Caroline Gouraud
Associate
Paris
+33 (0)1 76 70 40 34
cgouraud@reedsmith.com

Munich

Andy Splittgerber
Partner
Munich
+49 (0)89 20304 152
asplittgerber@reedsmith.com

Thomas Fischl
Counsel
Munich
+49 (0)89 20304 178
tfischl@reedsmith.com

Christian Leuthner
Senior Associate
Munich
+49 (0)89 20304 191
cleuthner@reedsmith.com

Alexander Hardinghaus
Associate
Munich
+49 (0)89 20304 134
ahardinghaus@reedsmith.com

Sven Schonhofen
Associate
Munich
+49 (0)89 20304 158
sschonhofen@reedsmith.com

Athens

Anthony Poulopoulos
Partner
Athens
+30 (0)210 41 99 423
apoulopoulos@reedsmith.com

Doretta Frangaki
Associate
Athens
+30 (0)210 41 99 425
dfrangaki@reedsmith.com

Thought Leadership

For more insight into the GDPR and other Data and Technology related matters, please take a look at our blog, the ***Technology Law Dispatch***, at:
www.technologylawdispatch.com

Recognition

Our team has been recognised over a number of years with rankings in both the ***Chambers*** and ***Legal 500*** directories.

"The team is responsive and approachable, very helpful and makes an effort to keep us updated about the latest important developments."
Chambers & Partners 2017

Reed Smith is a global relationship law firm with more than 1,800 lawyers in 27 offices throughout the United States, Europe, Asia and the Middle East.

Founded in 1877, the firm represents leading international businesses, from Fortune 100 corporations to mid-market and emerging enterprises. Its lawyers provide litigation and other dispute-resolution services in multi-jurisdictional and high-stakes matters, deliver regulatory counsel, and execute the full range of strategic domestic and cross-border transactions. Reed Smith is a preeminent advisor to industries including financial services, life sciences, health care, advertising, entertainment and media, shipping and transport, energy and natural resources, real estate, manufacturing and technology, and education.

ABU DHABI
ATHENS
BEIJING
CENTURY CITY
CHICAGO
DUBAI
FRANKFURT
HONG KONG
HOUSTON
KAZAKHSTAN
LONDON
LOS ANGELES
MIAMI
MUNICH
NEW YORK
PARIS
PHILADELPHIA
PITTSBURGH
PRINCETON
RICHMOND
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
SINGAPORE
TYSONS
WASHINGTON, D.C.
WILMINGTON

reedsmith.com