The General Data Protection Regulation: Three months to go

February 2018

ReedSmith

Driving progress
through partnership

Contents

The background

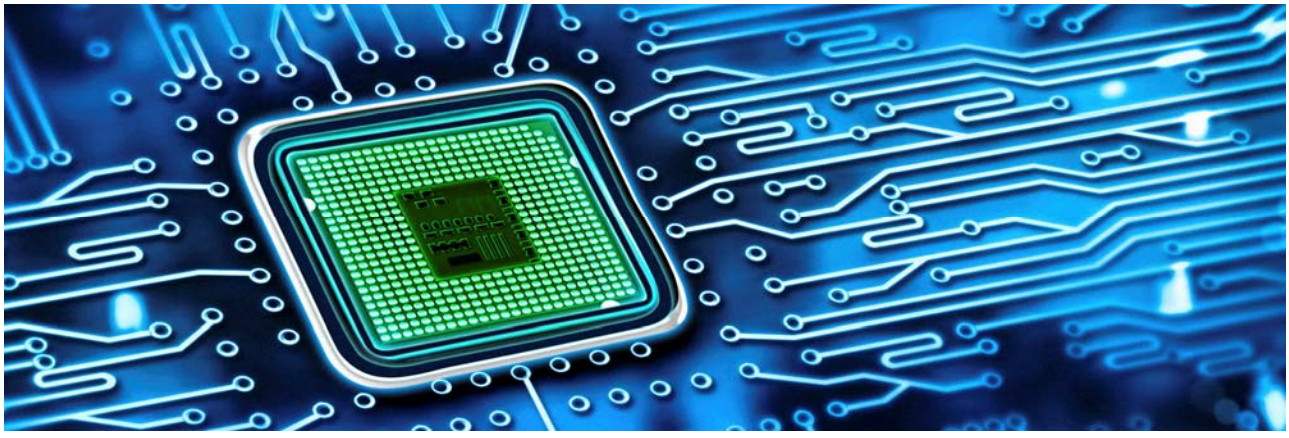
For a little more than 20 years, the protection of individuals in relation to the collection, use and processing of their personal data has been governed in Europe by the Data Protection Directive (95/46/EC) (the Data Protection Directive) adopted and implemented in national law by all 28 EU member states.

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 27 April 2016 and published in the Official Journal of the European Union 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.

This is now only three months away, so we wanted to update you on how to use this time to your advantage. With this in mind, we have produced this mini-guide using our experience from GDPR projects we've been guiding our clients on, and providing answers to some of the questions we are most frequently asked. Where you see a speech bubble, these are comments and questions gathered directly from our clients during a GDPR planning event held in London 23 November 2017.

We hope you find this guide useful; however, if you would like further information, please get in touch with one of our below key contacts for GDPR queries, or with any of our global team members included within this guide.



Why comply?

The new regulation will require organisations to implement and comply with a multitude of new obligations. Organisations will be required to produce documentary evidence of compliance, honour new rights for individuals, and be exposed to increased sanctions at up to 4 per cent of worldwide annual turnover, as well as group (class) actions. A few areas to note are detailed further below.

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.

Increased powers of enforcement

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 million 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.

Supply chain accountability and due diligence

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.

Data protection: design or default?

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.

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 path to GDPR compliance

The path to compliance involves 10 steps you should be aiming to complete between now and 25 May 2018:

- **Stakeholder awareness:** Embed data protection across your business functions
- **Data inventory:** Assess and record your data processing activities
- **Gap analysis:** Identify what needs to be updated or newly introduced to comply with the GDPR compliance requirements
- **Implementation plan:** Create a compliance programme to address the compliance gaps
- **Governance/data protection officer:** Assess whether the appointment of a DPO is necessary, and create a governance structure to support accountability requirements
- **Supply chain/processors:** Ensure supplier contracts contain adequate provisions to meet GDPR requirements
- **Cross-border data transfers:** Review legal mechanisms for cross-border data transfers from the EEA
- **Accountability processes:** Prepare tools and processes to document and implement compliance
- **Data subjects' rights:** Prepare policies and procedures to ensure requests to exercise rights can be handled effectively
- **Data breach notification:** Prepare a policy handling data breaches and notification requirements

What should your organisation be considering now, with three months to go?

1. Data inventory, gap analysis and implementation plan
2. Data protection impact assessments (DPIAs)
3. Data protection by design or by default?
4. Data breach notifications and breach response planning
5. Supply chain

Data protection officers

While some organisations can voluntarily 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**.

Top tips

- Appoint on a country or enterprise level
- Remember it can be tricky to terminate DPOs
- Do not over-appoint. Consider appointing stewards, chairpersons or local data champions.
- Ensure strong governance structure in place that can support the DPO if appointing a single DPO

Data subject rights

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 may be overridden where the controller implements appropriate safeguards.
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.

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
- Ensures 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
- Makes available all information necessary to demonstrate compliance with their obligations

Approaches to amending existing supply contracts

- We have found that many organisations are struggling with the process of amending their existing arrangements with suppliers. If existing supply agreements need to be amended, four main approaches can be adopted:
  - A number of the big suppliers are issuing their own set of GDPR-compliant supply agreement terms, which you could agree to.
  - You could agree a new Data Protection schedule with the supplier which could be appended to the existing agreement.
  - You could issue a letter agreement that seeks to amend the existing contract, and ask the supplier to sign and return the letter.
  - Where there is a compliance-with-all-laws clause in your supply agreement, you could take the aggressive approach of issuing a letter which states that as a result of a change in the law - i.e., the introduction of the GDPR – you believe that the contract should be amended in certain ways, and that the continued provision of services by the supplier constitutes acceptance by performance of those new terms.
- The approach that you should adopt will depend on a number of factors, including the importance of the contract, the length of the remaining term of the contract, and type of data that is being processed.

Data breach notification

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

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 – **within 72 hours**
- Individuals affected where the breach would likely result in a high risk to their rights and freedoms – **without undue delay**

A prime area for litigation

The UK has no requirement for security standards, but recognises and encourages the use of standards. **ISO 27001** should be considered the minimum standard.

Top tips

- There are artificial intelligence tools which recognise data breach in real time
- Consider a full data breach plan
- Train staff on how to respond to data breach
- In event of a breach, report to a DPO internally

Cross-border 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:

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.

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.

Specific derogations

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

Our global team

As part of the IP, Tech & Data 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 contacts around the world. Our global team consists of over 90 lawyers across our offices in Europe, the United States, Asia and the Middle East.

London

Cynthia O'Donoghue
Partner
International Head, IP, Tech & Data
London
+44 (0)20 3116 3494
codonoghue@reedsmith.com

Philip Thomas
Partner
London
+44 (0)20 3116 3526
pthomas@reedsmith.com

Katalina Bateman
Associate
London
+44 (0)20 3116 2866
kbateman@reedsmith.com

Karen Lust
Associate
London
+44 (0)20 3116 3925
klust@reedsmith.com

John O'Brien
Associate
London
+44 (0)20 3116 3485
jobrien@reedsmith.com

Curtis McCluskey
Associate
London
+44 (0)20 3116 3467
cmccluskey@reedsmith.com

Kirill Albrecht
Associate
London
+44 (0)20 3116 3476
kalbrecht@reedsmith.com

Ellie Brooks
Associate
London
+44 (0)20 3116 3657
ebrooks@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
Partner
Munich
+49 (0)89 20304 178
tfischl@reedsmith.com

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

Friederike Detmering
Associate
Munich
+49 (0)89 20304 111
fdetmering@reedsmith.com

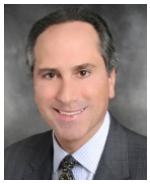
Sven Schonhofen
Associate
Munich
+49 (0)89 20304 158
sschonhofen@reedsmith.com

Athens

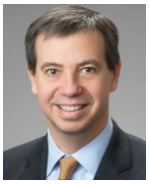
Anthony Poulopoulos
Partner
Athens
+30 (0)210 41 99 423
apoulopoulos@reedsmith.com

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

United States



Mark Melodia
Partner
Co-Leader, IP, Tech & Data
New York
+1 212 205 6078
mmelodia@reedsmith.com



Bart Huffman
Partner
Houston
+1 713 469 3874
bhuffman@reedsmith.com

Gerard Stegmaier
Partner
Washington D.C.
+1 202 414 9293
gstegmaier@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 dynamic international law firm, dedicated to helping clients move their businesses forward.

Our long-standing relationships, international outlook, and collaborative structure make us the go-to partner for speedy resolution of complex disputes, transactions, and regulatory matters.

This document is not intended to provide legal advice to be used in a specific fact situation; the contents are for informational purposes only.
"Reed Smith" refers to Reed Smith LLP and related entities. © Reed Smith LLP 2018

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