ReedSmith

Driving progress
through partnership

IT, Privacy & Data Security

Implementing GDPR Compliance

The General Data Protection Regulation: A Year to Go

June 2017

Contents

Background

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 (GDPR or 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 GDPR. which 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.

This is now only a year 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, as well as 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 on 23 May 2017.

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

Key European contacts

Cynthia O'Donoghue
Partner
London
+44 (0)20 3116 3494
codonoghue@reedsmith.com

Cynthia leads the International Information Technology, Privacy & Data Security team and is a partner in the IP, Tech & Data Group. Cynthia specialises in technology, data, cyber and commercial law, and has already advised a wide range of clients across the globe on the development and implementation of GDPR compliance programmes. Cynthia has particular experience advising clients in the financial services, life sciences and technology sectors.

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

Andreas is a partner in the IP, Tech & DataGroup, specialising in IT law, data protection/privacy, social media law and internet law (Germany and EU). He is passionate about technology and privacy and has also advised a significant number of clients in Germany and beyond on the GDPR. Andreas has particular experience advising clients in the entertainment and media, and retail and consumer sectors.

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

Daniel is a partner in Reed Smith's Paris office and works in French, English and German for clients across a broad range of sectors in the fields of compliance, data protection and commercial law, as well as litigation. Daniel has particular experience in the life sciences industry and regularly advises clients operating in that sector on data-related issues.

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 (i.e., class) actions. A few areas to note are detailed further below.

The long arm of the law

The GDPR applies to data 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's or processor's premises and equipment
- Issue warnings and formal 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 seen in the Data Protection Directive but was not anchored as a legal requirement in such explicit terms as we see now. As with several aspects of the GDPR, however, 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 (i.e., 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.

Data protection by design or by 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 many of the 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.

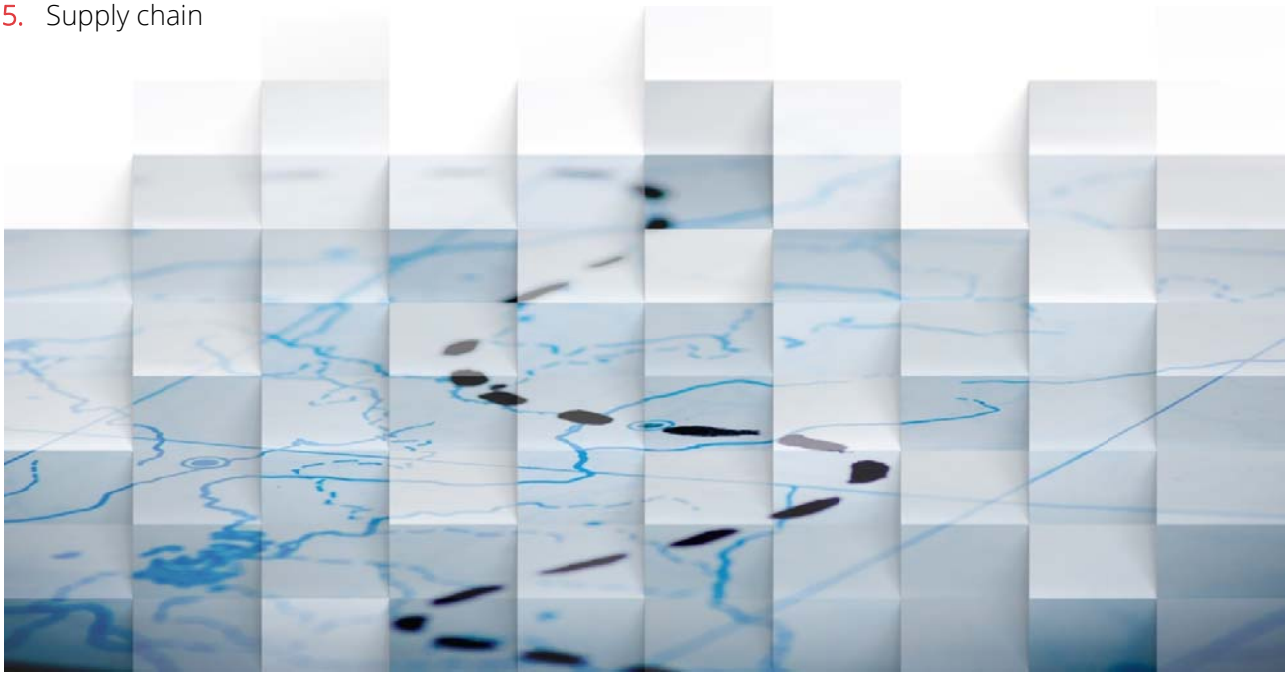
The path to GDPR compliance

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

1. **Stakeholder Awareness:** Embed data protection across your business functions
2. **Data Inventory:** Assess and record your data processing activities
3. **Gap Analysis:** Identify what needs to be updated or newly introduced to comply with the GDPR compliance requirements
4. **Implementation Plan:** Create a compliance programme to address the compliance gaps
5. **Governance/Data Protection Officer (DPO):** Assess whether the appointment of a DPO is necessary and create a governance structure to support accountability requirements
6. **Supply Chain/Processors:** Ensure supplier contracts contain adequate provisions to meet GDPR requirements
7. **Cross-Border Data Transfers:** Review legal mechanisms for cross-border data transfers out of the EEA
8. **Accountability Processes:** Prepare tools and processes to document and implement compliance
9. **Data Subjects' Rights:** Prepare policies and procedures to ensure requests to exercise rights can be handled effectively
10. **Data Breach Notification:** Prepare a policy handling data breaches and notification requirements

What should your organisation be considering now, with a year 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 inventory

Data inventory and gap analysis involves identifying the data you hold and how you use it, mapping your processes against the GDPR requirements to identify compliance gaps, and mapping out a plan to bridge the gaps. This is the basis for the rest of your year's compliance activity.

Data inventory – why?

Organisations should be conducting a data inventory as a basis for their GDPR preparation in order to identify gaps and have the necessary information in place for GDPR accountability requirements relating to data inventory, information documents, DPIAs, IT security risk analysis, data breach response plans and more.

Your collection of information (via questionnaires, online tools or 'data parties') should cover the following questions:

- What data do you have and/or process?
- What do you already know you are doing – i.e., what applications use the data, and what other consents and legal basis do you have?
- What documentation is in place?

If you start out with a lot of detail in your inventory, you will need to maintain that same level of detail subsequently.

It may be best to initially carry out your inventory on a large scale, later keeping only those 'buckets' of data that you need going forwards.

"It is a huge effort to maintain an accurate inventory; even with a fairly mid-level granularity, things may change and then the process needs to be done again."

A good template would be to carry out a general audit twice a year, where you can take stock and look at what is there. Then, when a new system or feature, or a new kind of processing, is rolled out, your inventory can be updated. Conducting DPIAs will also help by feeding into the inventory to make the required changes.

"For the amount and volume of data processed, we take a practical view – where there is more sensitive data, we maintain a higher level of granularity and ensure that there are additional checks on accuracy."

This is a good approach – the level of granularity of your inventory should always match the needs of your organisation and take into account the different types of data you hold and process.

"For my organization, data inventory would amount to a specific IT project, so there is not any real clarity on what budget this should come out of. All departments need to be involved, not just Legal and HR."

A lot of our clients are using IT budgets to carry out their data inventories. Legal and compliance teams need to stand over your GDPR programmes to drive forward the additional compliance required.

Data protection impact assessments (DPIAs), and data protection by design or by default

DPIAs

A data protection impact assessment (DPIA) is a process involving the identification, assessment and minimisation of data protection risks.

Data protection by design or by default

The GDPR also 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.

There are a lot of questions around what is meant by privacy by design, and what is required. Privacy should be in mind from the outset and continue throughout the complete life cycle of a project, product or process. It also helps organisations to meet obligations under the GDPR by ensuring processing is less likely to be intrusive and data subjects' rights and freedoms are upheld at all times.

Top tips

- **Policy procedures and standards should be in place within organisations to show how they are implementing technical and organisational practices (i.e., compliance training).**
- **For DPIAs, organisations must include details of the nature and purpose of the data, security, whether there are to be transfers, and whether these will be outside the EEA.**
- **Privacy by default is much simpler to achieve. It includes ensuring that there are no pre-ticked consent boxes, and that the strictest privacy settings are the default (e.g., for location data, the default is set to 'off' and the data subject is prompted with a pop-up to opt in).**
- **Privacy by design has to be implemented on a case-by-case basis. In apps, for example, it means that privacy choices and transparency are easily accessible. We recommend 'thinking out of the box' and using new technology and ideas to meet these requirements.**

Hot topic: GDPR and legal privilege

A number of clients have expressed concern in regards to maintaining legal privilege under a DPIA. We have laid out below some of the areas of concern and our experts' opinions.

The approach to take for now

A competition law approach should be taken; in other words, there is no legal privilege, as organisations are required to demonstrate compliance. Maintaining legal privilege may, therefore, put you in breach of certain principles under the GDPR as the two are fundamentally incompatible. In addition, legal privilege is not as uniformly interpreted across Europe as the GDPR.

"We want to maintain legal privilege as far as possible – litigation/regulatory privilege in particular."

Companies will struggle to meet legal requirements if a DPIA is done under legal privilege. How can you demonstrate compliance if there is legal privilege? The information needs to be kept available. While some parts of a DPIA could be kept under legal privilege, in general terms legal privilege is not possible.

"To what extent is it possible to keep legal privilege if your DPO is a qualified lawyer?"

Having a lawyer as a DPO can create issues in terms of conflict of interest – how can a DPO invoke privilege if they also have to police compliance within the organisation? The DPO should have a compliance/audit function, with support from the legal team as needed.

"It is difficult to maintain legal privilege – the people writing processes are from within the business. Lawyers review but do not have input."

DPIAs need to be as public as possible because companies need to demonstrate to the regulator that they are complying. There is nothing stopping companies from obtaining separate legal advice.

Security and data breach

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.

"We have struggled a lot with what to notify. In terms of security, it is important to always watch out for suppliers and processors, to ensure that a breach by them has as little impact as possible."

Suppliers should be contractually obliged to report to the controller within 24-48 hours of a breach incident, so that customers' data is not compromised.

"Some suppliers try to include wording like '72 hours of contractor becoming aware', which is making nonsense of the law."

Going forwards, it will be easier to incorporate notification-requirement wording in new supplier contracts.

"You have to work out what counts as personal data under the definition. So much is now deemed personal data, such as IP addresses. This is increasingly challenging in the online world."

Companies will have to make hard decisions about what is personal or not. Most people do not know how to change dynamic and static identifiers – you need to identify and mitigate these risks.

Top tips

- We have advised clients on potential data breaches. If you don't know whether personal data has been affected or whether there actually was a breach, it is best to take a cautious approach.
- It is important to build and maintain a relationship with regulators.
- It's not about individual employees; it's about respect for company data. You can have a raft of policies, but training is key. A lot of issues come up due to a lack of training, or where training is not pitched at the user level.

Compliance throughout the supply chain

The obligation to ensure sufficient guarantees of data protection across the supply chain is now anchored within the law, whereas it was not an explicit legal requirement under the outgoing directive.

Supplier due diligence

Controllers are required to carry out due diligence on suppliers (i.e., 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 to 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.

We asked our clients: what are you seeing in supply chain relationships?

"In large American organisations, it is hard to enforce obligations. We can't go ahead with agreements because the US are digging their heels in."

Top tips

- **We anticipate that many processors will expect new or enhanced obligations once the GDPR is fully in effect. It is important to maintain a consistent approach with suppliers.**
- **We recommend developing a suite of provisions, ranging from the compulsory provisions required by the Regulation to a fuller set of obligations, and tailoring the provisions on a case-by-case basis, using a risk-based approach.**

"We've started sending amended agreement wording to our suppliers. They are generally being understanding, but there are some sticking points."

Tools and processes

We have already helped a number of clients with the planning and implementation of their GDPR compliance programmes. As a result of this, we have developed tried and tested toolkits and created automated processes using AI and other technological tools to make the process as simple as possible.

Get in touch with one of the team to learn more about how we can help smooth the path to compliance for your organisation.

Thought leadership

Our team keep an eye out for updates and regularly post insight pieces looking at the GDPR and other data and technology related matters to our blog, the *Technology Law Dispatch*. Read these posts by subscribing for updates at: **www.technologylawdispatch.com**

An award-winning team

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

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

Selected as part of the inaugural Privacy and Consumer Protection: Practice Group of the Year
Law360

Ranked in Technology: Data Protection and Privacy
The Legal 500 U.S.

Ranked in Data Protection: UK-wide
The Legal 500 UK

Selected as 2015 Firm of the Year for Data Protection and Privacy
The Legal 500 U.S.

A global team you can trust

London

Cynthia O'Donoghue
Partner
+44 (0)203 116 3494
codonoghue@reedsmith.com

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

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

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

Munich

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

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

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

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

Paris

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

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

Athens

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

United States

Mark Melodia
Partner
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

Frequently asked questions

Does the GDPR cover just data of EU citizens or any personal data transferred out of the EU by an establishment (including data of a U.S. citizen)?

The GDPR applies when goods or services are offered to EU citizens or when the behaviour of EU citizens is monitored or tracked through the use of technology. It means that organisations which do not have an establishment in the EU are now subject to data protection regulation pursuant to the GDPR when they process the personal data of EU citizens. However, cross-border data transfers concerning a U.S. citizen would not fall under the scope of the GDPR. Because an establishment in the EU is regulated under the GDPR, U.S. citizens' data processed by and transferred to a third party, including intra-company, will be subject to the GDPR.

When would a U.S. company have to appoint a DPO? Could the U.S. company use the DPO of its UK affiliate?

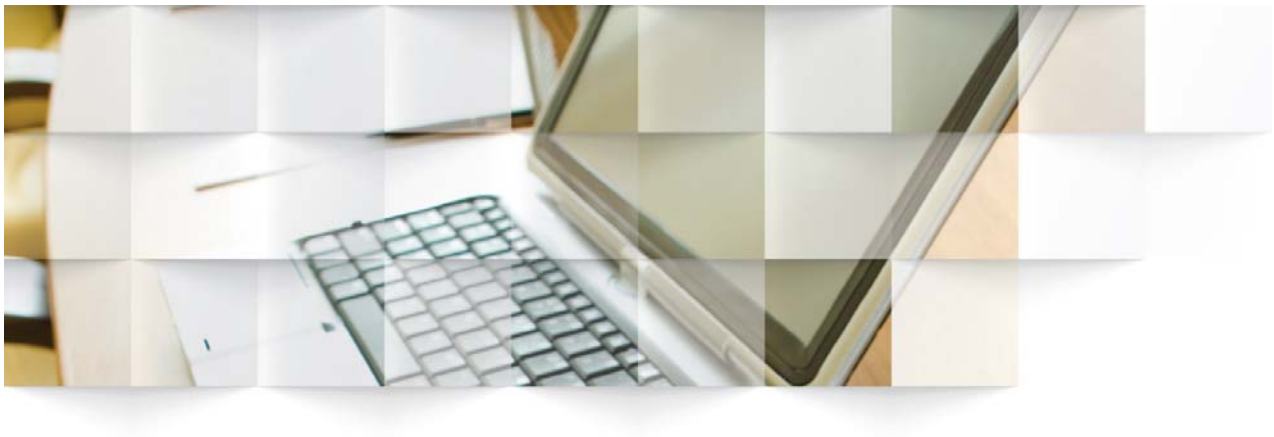
Any company handling EU citizens' data, whether or not that company is located in the EU, must designate a DPO if the company – as a core activity – monitors individuals systematically and on a large scale or processes special categories of personal data on a large scale. The DPO could be appointed as group DPO or on a part-time basis.

As privacy by design and default is fundamental, how might COs at financial firms, among others, comply with the GDPR when conducting monitoring of staff internal/external emails, etc. to ensure mandated supervision to prevent or stop insider dealing, etc.?

Privacy by design (PbD) means that an organisation needs to be able to show that it has adequate security in place and that compliance is monitored whereas privacy by default simply means that the strictest privacy settings automatically apply. In practice, it means that the IT department must take data protection principles into account when developing any form of product or service, or at the start of a new IT initiative or migration to a new system. PbD is meant to cover the entire life cycle of the processing, from collection, use, disclosure, transfer and handling to deletion, and includes consideration of security safeguards, confidentiality of the data, etc. In relation to monitoring of staff internal/external emails, other laws, in particular local labour and employment laws, are likely to apply as well.

Please could you confirm what BCRs are?

Binding corporate rules (BCRs) are a code of practice for intra-company, cross-border transfers of personal data that have the advantages of being binding and enforceable. BCRs are explicitly recognised in the GDPR and are available for both controllers and processors.



Reed Smith is a global relationship law firm with more than 1,700 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