The General Data Protection Regulation
A survival guide

Version 2.0
A new era

The General Data Protection Regulation now applies to the whole of the European Union. It marks the biggest shake up to European privacy laws for twenty years.

It has brought a number of changes, including new or stricter obligations for businesses, new or reinforced rights for individuals and enhanced enforcement powers for regulators. It is too early to assess the full impact of these changes, but the GDPR has clearly bolstered the importance of data protection and privacy rights.

An immediate change is greater public awareness of data protection, evidenced by a surge in individuals seeking to exercise their rights under the GDPR (some regulators are reporting a doubling in the number of complaints brought by individuals) and increased activism by privacy groups. Your customers, employees and other individuals expect more of you in a post-GDPR world.

The GDPR will also be supplemented by a new Regulation on Privacy and Electronic Communication. This was due to have been adopted in May 2018, to match up with the start of the application of the GDPR, but is now unlikely to be finalised until 2019 if not later.

This guide provides an overview of the GDPR, including details of the key changes it brings about. We have also included details extracted from relevant EU guidance and answers to many of the questions we have received from our clients about the GDPR.

We hope you find it useful.

Tanguy Van Overstraeten
Global Head of Data Protection
Tel: +32 2 501 94 05
tanguy.van_overstraeten@linklaters.com

Richard Cumbley
Global Head of TMT/IP
Tel: +44 20 7456 4681
richard.cumbley@linklaters.com

Dr Daniel Pauly
Partner
Tel: +49 69 710 03 570
daniel.pauly@linklaters.com
The GDPR at a glance

Question 1. Am I subject to the GDPR?

The GDPR applies primarily to businesses established in the EU or inextricably linked to such a business. However, it also applies to businesses outside the EU that:

- offer goods or services; or
- monitor individuals in the EU.

See Extra-territorial reach

Question 2. Am I processing personal data?

Processing is a very broad term and includes collecting, storing and using personal data.

Personal data means information that relates to an identified or identifiable living individual. This includes online identifiers, such as cookies, if they relate to an identified individual.

See Core rules and key concepts

Question 3. Am I a controller or processor?

A controller is a person that determines the purpose and means of the processing.

A processor is a person who simply acts on the instructions of the controller. For example, a payroll company or cloud hosting company.

Note, it is possible to be a joint controller.

See Core rules and key concepts

You are a processor

Processors are subject to a limited subset of obligations.

Data security

Personal data must be held securely. Processors need to notify controllers about personal data breaches.

See Data security and breach notification

Data protection officers

If you conduct some types of high risk processing, you must appoint a statutory data protection officer.

See Data protection officers

Record keeping and impact assessments

Under the GDPR, processors must keep records about their processing.

See Accountability and impact assessments

International transfers

The GDPR contains restrictions on when personal data can be transferred outside the EEA.

See International transfers
## You are a controller

### General processing principles
As a controller you must comply with all six general processing principles, namely:
- a. Fair and lawful processing
- b. Purpose limitation
- c. Data minimisation
- d. Data accuracy
- e. Storage limitations
- f. Data security

Accountability means that you must not only comply with these principles but be seen to comply.

See [Core rules and key concepts](#)

### Processing conditions
As a controller you must ensure your processing satisfies at least one processing condition, namely:
- a. Consent
- b. Performance of a contract
- c. Compliance with a legal obligation
- d. Protecting vital interests
- e. Public interests and functions
- f. Legitimate interests

There are strict controls on when valid consent can be obtained.

See [Processing conditions and Consent and children](#)

### Privacy notices
Under the GDPR you must tell individuals how you use their personal data. This is typically done through a privacy notice.

See [Privacy notices](#)

### Individuals’ rights
The GDPR preserves existing rights for individuals and adds additional rights such as the right to data portability and the right to be forgotten.

See [Individuals’ rights](#)

### Processor contracts
Where you use a processor, you must have a contract with them containing certain additional terms such as a right to audit.

See [Processors](#)

### Data protection officers
If you conduct some types of high risk processing, you must appoint a statutory data protection officer.

See [Data protection officers](#)

### Sensitive personal data
Information about criminal offences and special category personal data (such as health information) can only be processed in limited circumstances.

See [Processing conditions](#)

### Data security and breach notification
Personal data must be held securely. Where a data breach occurs, you may have to tell the regulator and affected individuals.

See [Data security and breach notification](#)

### Record keeping and impact assessments
Under the GDPR, you must keep new records about your processing. In addition, if you undertake a new high risk project, you must conduct a formal impact assessment.

See [Accountability and impact assessments](#)

### International transfers
The GDPR contains restrictions on when personal data can be transferred outside the EEA.

See [International transfers](#)
Contents

The GDPR at a glance 4
Contents 7
Extra-territorial reach 8
Core rules and key concepts 11
Processing conditions 18
Consent and children 22
Individuals’ rights 26
Privacy notices 30
Accountability and impact assessments 33
Data protection officers 36
Data security and breach notification 38
Processors 42
International transfers 46
Sanctions 50
National law and regulators 52
Summary 58
Glossary 60
Contacts 61
Extra-territorial reach

Inside the EU – Establishment
The GDPR primarily applies to businesses established in the EU. Establishment means an effective and real exercise of activity through stable arrangements in the EU. The legal form of the establishment is not a determining factor and it could be a branch or a subsidiary. It also doesn’t matter where the actual processing takes place; what matters is where the entity taking decisions about the processing is based.

This is broadly similar to the test under the old Data Protection Directive, as set out by the Court of Justice in Weltimmo (C-230/14) that “even a minimal” establishment is sufficient. This interpretation is not expressly carried over to the GDPR but the draft guidelines from the Board confirm the Weltimmo test applies and the threshold for an establishment is “quite low”. However, it is not without limits. For example, merely having a website available in the EU is not an establishment, nor is simply using an EU processor.

Outside the EU – Offering
The GDPR also contains new provisions to expressly extend the reach of European data protection laws to businesses based outside the EU. Controllers and processors will be caught where the processing activities relate to the offering of goods or services to individuals in the EU.

This is based on the “directed at” test in the Rome I and Brussels Regulation, meaning that existing case law on this test will be relevant (see When do you offer goods or services to individuals in the EU?). It captures both free and paid-for goods and services.

This extra-territorial provision only applies the GDPR to personal data about individuals physically present in the EU at the time the offer takes place, though the nationality or habitual residence of those individuals is irrelevant. The GDPR does not apply to personal data processed about other individuals.

Outside the EU – Monitoring
There is also an express territorial extension to businesses that monitor the behaviour of individuals in the EU. The GDPR does not contain much guidance on what this means though the recitals refer to individuals being tracked on the internet for profiling purposes.

The draft guidelines from the Board provide some useful insight into the scope of this provision:

> Targeting. While there is no express requirement in the GDPR that monitoring activities “target” individuals in the EU, the Board’s draft guidelines suggest that this should be implied and the monitoring activity must be for the specific purpose of monitoring individuals in the EU.
Extra-territorial reach

When do you offer goods or services to individuals in the EU?

This test is similar to the “directed at” test used in relation to consumer contracts in the Brussels Regulation and the Rome I Regulation.

The mere accessibility of your website by individuals in the Union or use of the languages of one of the Member States in the EU (of the same as the language of your home state) should not by itself make you subject to the GDPR. However, the following factors are a strong indication that you are offering goods or services to individuals in the Union and so are subject to the GDPR:

Language - You are using the language of a Member State and that language is not relevant to customers in your home state (e.g. the use of Hungarian by a US website).

Currency - You are using the currency of a Member State, and that currency is not generally used in your home state (e.g. showing prices in Euros).

Domain name - Your website has a top level domain name of a Member State (e.g. use of the .de top level domain).

Delivery to the Union - You will deliver your physical goods to a Member State (e.g. sending products to a postal address in Spain).

Reference to citizens or Member States - You use references to individuals in a Member State, or the Member State itself, to promote your goods and services (e.g. if your website talks about Swedish customers who use your products).

Customer base - You have a large proportion of customers based in the Union.

Targeted advertising - You are targeting advertising at individuals in a Member State (e.g. paying for adverts in a French newspaper or paying for search engine adverts to be directed to individuals in Denmark).

Inherently international - Your activities are inherently international (e.g. offering holidays in exotic locations to foreign tourists). This would be a strong indicator if you offered travel instructions from a Member State to that jurisdiction.

Member State addresses – You offer an address or local telephone number in a Member State or the telephone numbers on your website have an international prefix.

Importantly, this is not a binary analysis. The question is not whether a single criterion is met but whether a cumulative assessment of these criteria point to an intention to offer goods or services to individuals in the EU.

In the event of an investigation, a business’ internal discussions will be relevant, as well as these external objective factors. Does the business “envisage the offering of services to” individuals in the Union?

Subsequent profiling. In addition, simply collecting or analysing personal data about individuals in the EU may not automatically constitute monitoring. You should also consider if the controller is subsequently carrying out behavioural analysis or profiling on that personal data.

Relevant activities. Finally, the draft guidelines provide a list of the sort of activities that are likely to be “monitoring”, namely: (a) behavioural advertising; (b) location tracking; (c) online tracking using cookies; (d) personalised diet services; (e) CCTV; (f) market surveys; and (g) monitoring health.

Again, the monitoring test only captures personal data about individuals physically present in the EU at the time the monitoring takes place.

Processors

The Board’s draft guidelines also contain a number of helpful clarifications about the application of these provisions to processors.

Where a non-EU controller uses an EU processor, the EU processor will not constitute an establishment of the non-EU controller. In other words, this alone will not bring the non-EU controller into the scope of the GDPR (see above).

1 Recital 22.
2 See the European Data Protection Board’s Draft guidelines on the territorial scope of the GDPR (3/2018). Article 3.
3 Article 3(2).
4 Recital 23, Emrek v Sabranovic (C-218/12) and the joined cases of Pammer v Reederei (C-585/05) and Hotel Alpenhof v Heller (C-144/09).
5 It is worth noting the UK Information Commissioner has already served an Enforcement Notice on AggregatelQ Data Services Limited on the basis it is monitoring individuals in the UK.
6 Recital 24.
7 Unless the controller is caught by the offering or monitoring test. Interestingly, the draft guidelines also state that the processor should not conduct processing that “entails inadmissible ethical issues”, suggesting there is some control over the substantive processing, but the legal basis for this assertion is not clear.
8 Recital 23.
The EU processor must still comply with its obligations under the GDPR (see Processors) but the substantive processing largely falls outside the scope of the GDPR. One unanswered question is how the EU processor can comply with the controls on transborder dataflow when transferring personal data back to the controller (see International transfers). In the majority of cases there would be no clear legal basis for this transfer.

Where an EU controller uses a non-EU processor, the EU controller will need to ensure a processor contract is in place and would need to comply with the controls on transborder dataflow, likely through the use of Model Contracts. However, there is no suggestion that the non-EU processor will become directly subject to the GDPR under this arrangement.

Appointment of a representative

Where the offering or monitoring tests apply, the controller or processor must appoint a representative. That representative must be based in a Member State in which the relevant individuals are based. There is a limited exemption to the obligation to appoint a representative where the processing is occasional, is unlikely to be a risk to individuals and does not involve large scale processing of sensitive personal data.

It is not clear what liability representatives have under the GDPR. The recitals suggest that enforcement action can be taken against a representative, and the draft guidelines from the Board state that the purpose of the representative is to allow the local enforcement, in other words to allow supervisory authorities to impose fines and penalties directly on representatives. This appears to be based on the assumption the representative can then recover those fines from the relevant controller based on an indemnity in their appointment contract.

However, there is no operative article to this effect. This might be largely a question of national law. For example, under the UK Data Protection Act 2018 representatives must respond to information notices, failing which they can be subject to administrative fines.

In any event, it’s not clear why anyone would want to act as a representative. It may be possible to “persuade” a group company to take on the role or set up a special purpose vehicle in the EU, but, even then, the group company will need to consider if it is really in its interests to take on this role.

Similarly, some third party service providers are prepared to take on the role. However, they will normally want to be paid given the risks they undertake and are likely to want significant protection against any liability they incur, including appropriate insurance and indemnity cover.

FAQ

Are there any third parties that will act as representative?

There are a number of third parties now offering to act as an EU representative. The cost and terms under which they provide that service vary. We do not act as an EU representative.

EU guidance

The European Data Protection Board’s Draft guidelines on the territorial scope of the GDPR (3/2018).

These guidelines are in draft and are open to consultation until 18 January 2019. They will be finalised at some point after that and may take a different position on some issues.

To do

- Evaluate if your business (if established outside the EU) is caught by the GDPR.
- Consider if you want to take steps to avoid being subject to the GDPR, eg avoid dealing with individuals in the EU.
- If you are established outside the EU but caught by the GDPR, identify and appoint a representative in the EU (unless exempt).

---

9 Article 3(1).
10 Article 27.
11 Recital 80.
12 Section 142(9) and 155(1)(b), Data Protection Act 2018.
Core rules and key concepts

The GDPR preserves most of the core rules in the old Data Protection Directive. Technology has changed significantly in the last twenty years, with the emergence of the internet, social media and smartphones. However, the GDPR preserves most of the core rules in the Data Protection Directive, which was adopted in 1995; namely a set of broad, technology neutral principles. This principle-based approach has the advantage of being flexible and capable of adapting new technology. The disadvantage is that it is not always clear how it applies to a particular situation.

Single market
One of the key aims of the GDPR is to support the digital single market by creating a level playing field in all Member States. This is a key reason why the GDPR is an EU Regulation and therefore directly effective in all Member States. However, there is still scope of substantial divergences between Member States in a number of areas (see Full harmonisation still some way off).

Processing personal data
The GDPR applies to the processing of personal data (see Key concepts). Processing is a broad concept and includes not only collecting or disclosing personal data but also activities such as use, storage or destruction.

Personal data is information that relates to an identified or identifiable living individual. This is also a broad term. It includes a wide range of information. While the GDPR extends the definition of personal data to include online identifiers, such as cookies or IP addresses, this was already likely to be the case. However, the GDPR only applies to personal data if it is processed wholly or partly by automated means or is part of a sophisticated hard copy filing system. It does not apply to ad hoc paper records.

Sensitive personal data
The GDPR identifies certain types of information as ‘special category’ personal data, being personal data that requires additional justification to process (see Processing conditions). Special category personal data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. The inclusion of genetic and biometric information is new and were not characterised as special category personal data under the Data Protection Directive. The GDPR also contains additional restrictions on the processing of personal data relating to criminal convictions and offences.

Key points
- The GDPR retains the same core rules as the old Data Protection Directive.
- It regulates the processing of personal data. Those processing personal data do so as a controller or a processor. A processor just acts on the instructions of the controller.
- All processing must comply with six general processing principles. These principles are similar to those in the Data Protection Directive.
- The concept of sensitive personal data has been retained and expanded to include genetic and biometric data.

FAQ
So nothing has really changed?
The core rules are broadly the same. The GDPR will look quite familiar to experienced privacy practitioners. But this is a trap for the unwary; there are some significant changes. In addition, the GDPR adds a number of important new obligations, highlighted elsewhere in this guide. Finally, there is a significant increase in the sanctions for getting it wrong.

13 Breyer (C-580/14).
14 Article 2(1).
15 Article 9.
Controller

The majority of the obligations under the GDPR fall on the person that determines the purpose and means of the processing – the “controller”. Controllers must:

> satisfy all six general processing principles (see General processing principles); and

> satisfy a relevant processing condition (see Processing conditions).

The controller can either act independently or jointly with other controllers. Where the controller acts jointly with others, they need an arrangement to allocate responsibilities for compliance with the GDPR. 16 This will typically be through a joint controller agreement.

Processor

In contrast, a processor simply acts on the instructions of the controller. As a result, processors are subject to a much more limited set of obligations, mainly limited to security and record keeping (see Processors).

What are you?

Deciding if the third party you disclose personal data to acts as controller or processor is not always straightforward. The GDPR imposes a binary dichotomy but, in practice, the distinction is often more fluid:

> Clearly a controller – Some third parties will obviously be a controller. For example, once you give personal data to a tax authority you lose control. The tax authority is obviously a controller.

> Clearly a processor – Some third parties will obviously be a processor. For example, if you purchase data storage in the cloud, the cloud provider will very likely be a processor. It can only use that data on your instructions and has no right to use it for its own purposes.

> In between – Between these two extremes, there is a grey area in which it may not be clear if someone acts as independent controller, joint controller or processor. In most cases, the best solution is for the parties to decide on the capacity in which they both act and document the relationship accordingly.

Controller or processor?

You provide personal data:

<table>
<thead>
<tr>
<th>You provide personal data:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; about your employees to a company that provides payroll services to you.</td>
<td>The payroll company is likely to act as processor.</td>
</tr>
<tr>
<td>&gt; about your customers to a company that sends out postal mailing on your behalf.</td>
<td>The mailing company is likely to act as processor.</td>
</tr>
<tr>
<td>&gt; about your employees to another company that is looking to buy your business.</td>
<td>The bidder is likely to act as controller.</td>
</tr>
<tr>
<td>&gt; about your customers to your lawyers to obtain legal advice.</td>
<td>Your lawyers are likely to act as controller.</td>
</tr>
<tr>
<td>&gt; about one of your employees to the police who are investigating a possible crime.</td>
<td>The police will act as controller.</td>
</tr>
</tbody>
</table>

Relevant case law

A number of recent cases looking at this issue have taken an expansive view of the controller concept.

For example, an education company with a “fan page” on Facebook was found to be joint data controller with Facebook in relation to personal data collected on that page because it “managed and promoted” the page. 17 This was the case even though the operator of the fan page had little, if any, practical ability to control, or even access, the personal data Facebook gathered about visitors to the page.

Similarly, the Jehovah’s Witness community was joint controller of personal data collected by its door-to-door preachers even though it had no access to that personal data. This was because it “organised, co-ordinated and encouraged” those activities. 18

Mixed roles

When carrying out this analysis, note that a party can process different pools of personal data in different capacities. For example, a cloud provider offering data storage will very likely act as processor in relation to stored data. However, it will likely act as controller in relation to the contact names and details of the customers who buy those cloud services.

Why does it matter?

The distinction between controller and processor is important as:

> Scope of obligations - The majority of the obligations in the GDPR fall on controllers, not processors.

> Processor contract - Where a controller provides personal data to a processor, it must put a processor contract in place (see Processors).

> Data “ownership” - From a commercial perspective, if a party acts as processor it will only be able to use that personal data on the controller’s behalf. The processor cannot use the personal data for its own purposes.


Core rules and key concepts

General processing principles

The key obligation under the GDPR is to comply with all six general processing principles when processing personal data (see table above).

These broad common-sense obligations are very similar to the processing principles under the old Data Protection Directive. Much of the existing guidance and understandings around these obligations will continue to apply.

These principles are supported by a general accountability obligation. This means you must not only comply but be seen to comply (see Accountability and impact assessments).

Pseudonymised data and other “risk based” concepts

While much of the GDPR is familiar, there are some important new concepts, including processing that is a “risk” to individuals or a “high risk” to individuals and “large scale” processing (see New concepts).

These provisions have been included in order to apply the GDPR in a proportionate manner that reflects the risk of the processing.

The GDPR also introduces the concept of “pseudonymised data”. This concept was originally proposed as a radical third class of data (neither personal nor anonymised) that would be regulated in a completely different way. Under the GDPR, it ends up as an important and useful privacy-enhancing mechanism, but does not materially change the core rules in the GDPR. Importantly, pseudonymised data is still a form of personal data.

---

The six general processing principles

A controller must ensure the processing of personal data complies with all six of the following general principles:

1. **Lawfulness, fairness and transparency** - Personal data must be processed lawfully, fairly and in a transparent manner;

2. **Purpose limitation** - Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (with exceptions for public interest, scientific, historical or statistical purposes);

3. **Data minimisation** - Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. **Accuracy** - Personal data must be accurate and, where necessary, kept up to date. Inaccurate personal data should be corrected or deleted;

5. **Retention** - Personal data should be kept in an identifiable format for no longer than is necessary (with exceptions for public interest, scientific, historical or statistical purposes); and

6. **Integrity and confidentiality** - Personal data should be kept secure.

---

16 Article 26.
17 ULD v Wirtschaftsakademie (C-210/16).
18 Tietosuojavaltuutettu (C-25/17).
Use of recitals

A final point to consider is the inclusion of substantive obligations in the recitals. For example, the rules on consent in the articles are relatively short and straightforward but are supplemented by numerous additional requirements in the recitals, such as a ban on the use of pre-ticked boxes and a ban on tying of consent to the performance of a contract (see Consent and children).

It is not entirely clear what effect these additional obligations have. The recitals to a Regulation have no binding legal force. They can be used to help interpret a rule (so long as it not contrary to its wording), but cannot themselves constitute a rule.

Some of the recitals in the GDPR test the boundaries of these principles. For example, where an entity is based outside the EU they must, in most cases, appoint a representative in the EU. The recitals state that enforcement action can be taken directly against a representative, but there is no corresponding provision in the articles of the GDPR. Does the lack of an operative article mean there is no direct liability for representatives? This question may well end up before the European Court of Justice.

Out of scope

Some types of processing fall outside the GDPR altogether. The GDPR does not apply to processing:

- by a natural person in the course of a purely personal or household activity. Private use of social networks is specifically identified as being exempt.
- by law enforcement agencies for the prevention or investigation of crimes or to protect public security. These entities will be subject to the Criminal Law Enforcement Data Protection Directive (2016/680);
- for activities that fall outside EU law (e.g., national security);
- for the purpose of the EU’s foreign and security policy; and
- by EU institutions. Those institutions are subject to Regulation 45/2001 on the processing of personal data by Community institutions.

To do

- Work out if you process personal data as controller or processor.
- When you provide personal data to third parties, work out if they are controller or processor.
- Ensure you comply with the six processing principles.
### Key concepts

**Personal data**

Personal data is:
1. information
2. relating to
3. an identified or identifiable
4. natural person.

It is a broad term and includes a wide range of information.

The GDPR expressly states this includes online identifiers such as IP addresses and cookie identifiers. However, this is already likely to have been the case under the Data Protection Directive (Breyer C-582/14).

**Special category personal data**

This is personal data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

The inclusion of genetic and biometric data is new.

Information about criminal convictions and offences is treated separately and can only be processed under the control of official authority or where authorised by EU or Member State law.

**Controller**

This is a person who, alone or jointly with others, determines the purposes and means of the processing of personal data.

In other words, the controller decides “what” personal data will be used for and “how” it will be done.

**Processor**

This is a person who processes personal data on behalf of a controller.

An example might be a company that processes your payroll or a cloud provider that offers data storage. However, in more complex relationships it can be difficult to work out if someone acts as controller or processor in practice. Unlike under the Data Protection Directive, processors will become directly liable for compliance with some parts of the GDPR.

**Data subject**

The data subject is the natural person to whom the personal data relates.

We refer to them as “individuals” in this report.

**Processing**

Processing is a very broad concept and includes almost anything you can do with personal data, including collection, use, storage and destruction.

Disclosure is one form of processing, but the definition is much wider than that.
# New concepts

## Pseudonymised data

**Relevance:** Pseudonymised personal data is not exempt from the GDPR. However, it may be easier to justify the processing of pseudonymised personal data. For example, the GDPR states this may justify the use of personal data for secondary purposes, or could be a means of implementing privacy by design or data security.

**Meaning:** Personal data that can no longer be attributed to a specific data subject without the use of additional information, that additional information being kept separately and securely. 28

---

## Risk to individuals

**Relevance:** This is an important concept that arises at several points in the GDPR. For example: (a) regulators do not have to be told about data breaches if they are unlikely to be a “risk” to individuals; (b) businesses with less than 250 employees are not exempt from record keeping requirements if their process is likely to be a “risk” to individuals; and (c) this is a factor in determining if businesses based outside of the EU, but caught by the GDPR, need to appoint a representative in the EU.

**Meaning:** There is a “risk” to individuals if processing could lead to physical, material or non-material damage. This includes profiling or processing that could lead to discrimination, identity theft, damage to reputation or reversal of pseudonymisation. 25 It includes any processing of sensitive personal data or personal data about children or other vulnerable persons or processing that involves large amounts of personal data. In the context of a personal data breach, risk will require an assessment of a range of factors including the type of breach, the nature and sensitivity of the data, the ease of identification of individuals, the severity of the consequences, the number of individuals affected and any special characteristics of the controller or the individuals (see Data security and breach notification).

---

## Large scale processing

**Relevance:** This concept is also a factor in determining whether obligations under the GDPR are triggered. For example: (a) businesses must appoint a data protection officer if they process sensitive personal data on a “large scale” or their core activities involve monitoring on a “large scale”; (b) businesses based outside the EU, but caught by the GDPR, must appoint a representative if they process sensitive personal data on a “large scale”; and (c) privacy impact assessments are needed if the processing involves sensitive personal data or monitoring public areas on a “large scale”.

**Meaning:** The GDPR suggests that it means processing a considerable amount of personal data at regional, national or supranational level which could affect a large number of data subjects. However, it does not include the processing of personal data about patients or clients by an individual physician or lawyer. Guidance from the Board suggests this involves an assessment of: (a) the number of data subjects affected; (b) the volume and range of personal data processed; (c) the duration of the processing activity; and (d) the geographic extent of the processing. 29

---

**Notes:**

25 Recital 75.
26 Article 29 Working Party’s Guidelines on personal data breach notification (WP 250 rev.01).
28 Article 4(5).
29 See the Article 29 Working Party’s Guidelines on data protection officers (WP 243 rev.01).
Processing conditions

Key points

Any processing of personal data must satisfy a statutory processing condition.

The choice of processing condition is important; it affects the obligations imposed by the GDPR and the rights available to individuals.

These processing conditions are similar to those under the old Data Protection Directive. However, it will be much harder to rely on consent.

The processing of special category personal data or information about criminal offences is only possible if additional conditions are satisfied.

Legitimate Interests

The legitimate interests condition involves a "careful assessment of" the underlying processing. It involves a three-step test:

1. What is the legitimate interest? You must identify the legitimate interests of the controller or another natural person. This requires an assessment of a range of factors such as the reasonable expectation of individuals, the nature and sensitivity of the processing and any safeguards to protect the individual’s interests.

2. Is the processing necessary? Do you have to use personal data to satisfy that interest? Is there a less intrusive way to achieve that aim?

3. Balancing test. Do the rights of individuals override your legitimate interest. This requires an assessment of a range of factors such as the reasonable expectation of individuals, the nature and sensitivity of the processing and any safeguards to protect the individual’s interests.

Given the subjective nature of this test, it will often be sensible to document your thought processes through a Legitimate Interests Assessment.

Processing conditions (Article 6(1))

The processing of personal data will only be lawful if it satisfies at least one of the following processing conditions:

a. Consent - The individual has given consent to the processing for one or more specific purposes. Consent will be much harder to obtain under the GDPR;

b. Necessary for performance of a contract - The processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual prior to entering into a contract;

c. Legal obligation - The processing is necessary for compliance with a legal obligation to which the controller is subject. Only legal obligations under EU or Member State law will satisfy this condition. However, that law need not be statutory (eg common law obligations are sufficient);

d. Vital interests - The processing is necessary in order to protect the vital interests of the individual or another natural person. This is typically limited to processing needed for medical emergencies;

e. Public functions - The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Those functions must arise under Member State or EU law; or

f. Legitimate interests - The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Public authorities cannot always rely on this condition.
<table>
<thead>
<tr>
<th>Processing Condition</th>
<th>Is processing based on the condition contestable?</th>
<th>Does it trigger the 'right to be forgotten'?</th>
<th>Does it trigger the data portability right?</th>
<th>Automated decision making allowed?</th>
<th>Does it trigger additional requirements for privacy notices?</th>
<th>Do you lose the 'one stop shop' mechanism?</th>
<th>Might you be exempt from Privacy Impact Assessments?</th>
<th>Other issues</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Art. 7(3)</td>
<td></td>
<td></td>
<td>Art. 17(1)(b)</td>
<td>Art. 20(1)(a)</td>
<td></td>
<td></td>
<td>Art. 8</td>
</tr>
<tr>
<td></td>
<td>Art. 6(1)(b)</td>
<td></td>
<td></td>
<td>Art. 17(1)(b)</td>
<td>Art. 20(1)(a)</td>
<td></td>
<td></td>
<td>No.</td>
</tr>
<tr>
<td></td>
<td>Art. 6(1)(c)</td>
<td></td>
<td></td>
<td>No.</td>
<td>Art. 17(3)(b)</td>
<td></td>
<td></td>
<td>Possibly.</td>
</tr>
<tr>
<td></td>
<td>Art. 6(1)(d)</td>
<td></td>
<td></td>
<td>No.</td>
<td>Art. 17(3)(b)</td>
<td></td>
<td></td>
<td>No.</td>
</tr>
<tr>
<td></td>
<td>Right to object applies.</td>
<td></td>
<td></td>
<td>Art. 17(1)(b)</td>
<td>Art. 20(1)(a)</td>
<td></td>
<td></td>
<td>No.</td>
</tr>
<tr>
<td></td>
<td>Right to object applies.</td>
<td></td>
<td></td>
<td>Art. 21(1)</td>
<td>Art. 17(1)(c)</td>
<td></td>
<td></td>
<td>No.</td>
</tr>
</tbody>
</table>

Is processing based on the condition contestable?
- Yes: Consent can be withdrawn.
- No: No.

Does it trigger the 'right to be forgotten'?
- Yes: Yes.
- No: No.

Does it trigger the data portability right?
- Yes: Yes.
- No: No.

Automated decision making allowed?
- Yes: Yes.
- No: No.

Does it trigger additional requirements for privacy notices?
- Yes: Yes.
- No: No.

Do you lose the ‘one stop shop’ mechanism?
- Yes: Yes.
- No: No.

Might you be exempt from Privacy Impact Assessments?
- Yes: Yes.
- No: No.

Other issues
- Restrictions on children consenting online.
- Cannot be used by public authorities. Can be difficult to use with children.

9 November 2016 linklaters.com
Special category personal data

The processing of special category personal data must satisfy an additional special category processing condition reflecting the private and sensitive nature of this information. For example, while the processing of normal personal data can be carried out with consent, the processing of special category personal data requires “explicit” consent.

This is an area in which there is relatively substantial national divergence between Member States. For example:

> Some Member States, such as the UK, have as part of their implementing legislation produced extensive (and exhaustive) lists of the circumstances in which special category personal data can be processed. These additional conditions mainly arise from Article 9(2) (g) which allows processing where it is in the substantial public interest and is based on EU or Member State law.  

> In contrast, other Member States (such as Germany) do not have extensive lists of additional processing conditions and instead rely on existing EU or Member State law as providing a justification. For example, the processing of special category personal data is permitted under the existing EU Anti-Money Laundering Directives without needing to be spelled out in national data protection legislation.

The private and sensitive nature of this type of data means that, in addition to satisfying a special category processing condition, it should be handled with care and its use minimised wherever possible.

Processing conditions - Special category personal data (Article 9(2))

The GDPR places much stronger controls on the processing of special category personal data. While there are a number of processing conditions, those conditions are narrower. Any processing of personal data must satisfy at least one of the following conditions:

a. **Explicit consent** - The individual has given explicit consent. However, EU or Member State law may limit the circumstances in which consent is available;

b. **Legal obligation related to employment** - The processing is necessary for a legal obligation in the field of employment and social security law or for a collective agreement;

c. **Vital interests** - The processing is necessary in order to protect the vital interests of the individual or another natural person. This is typically limited to processing needed for medical emergencies;

d. **Not for profit bodies** - The processing is carried out in the course of the legitimate activities of a not-for-profit body and only relates to members or related persons and the personal data is not disclosed outside that body without consent;

e. **Public information** - The processing relates to personal data which is manifestly made public by the data subject;

f. **Legal claims** - The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g. **Substantial public interest** - The processing is necessary for reasons of substantial public interest, on the basis of EU or Member State law;

h. **Healthcare** - The processing is necessary for healthcare purposes and is subject to suitable safeguards;

i. **Public health** - The processing is necessary for public health purposes and is based on EU or Member State law; or

j. **Research** - The processing is necessary for archiving, scientific or historical research purposes or statistical purposes and is based on EU or Member State law.

Member States can introduce additional conditions in relation to health, genetic or biometric data.

---

30 Recital 47.
31 Recitals 47-49.
32 Recital 47.
33 This is recommended in the UK, see the Information Commissioner’s Guide to the GDPR, Lawful basis for processing.
34 Articles 13(1)(c) and (d), 13(2)(c), 14(1)(c) and 14(2)(c) and (d).
35 Article 20 and 21.
36 Articles 6(1)(c), (e) and Article 55(2).
37 However, additional safeguards apply including the need to prepare an “appropriate policy”.
Processing conditions

Who is a public authority?

The GDPR applies a number of special rules to public authorities. For example, a public authority must appoint a data protection officer (see Data Protection Officers) and cannot rely on the legitimate interests test when performing its tasks. Under European law, a public authority is:

"a body, whatever its legal form, which has been made responsible, pursuant to a measure adopted by the State, for providing a public service under the control of the State and has for that purpose special powers beyond those which result from the normal rules applicable in relations between individuals". 38

It potentially includes not only the traditional emanations of the state, but also some private sector entities such as utility companies. However, some Member States have explicitly set out who is a public authority in their national legislation. 39

Information about criminal offences

Information about criminal convictions can only be used pursuant to EU or Member State law, or under the control of an official authority. 40 There are no other justifications. On the face of the GDPR, even consent from the individual will not provide a justification to process this type of personal data.

However, the position in practice varies greatly from Member State to Member State:

> Some such as Poland have included limited additional situations in which this information can be processed in their national legislation. For example, to permit employers to carry out criminal record checks on applicants.

> Some Member States have included comprehensive provisions allowing the processing of criminal information in a broad range of situations. For example, the UK allows information about criminal offences to be processed in much the same situations as special category personal data can be processed.

> Others have been more generous still. For example, in Austria information about criminal offences can be processed if there is a legitimate interest to do so.

Impact on public authorities

One significant change is that public authorities can no longer use the legitimate interests condition to process personal data “in the performance of their tasks”. 41 This condition is relied upon heavily in practice and its absence means that public authorities will have to rely on alternative processing conditions (such as the public functions condition). 42 It is not clear what impact this will have on commercial and other non-core activities. Are they in the public interest and, if not, how can the public authority justify that processing? What are the public authorities “tasks”? Is it everything they do or just what they are required to do by law? 43

The GDPR imposes more onerous obligations on public authorities in a number of other ways. For example, public authorities must always appoint a data protection officer (see Data protection officer). 44 They are also subject to greater restrictions when transferring personal data outside the EU. 45

Finally, the definition of public authority is potentially broad (see Who is a public authority?).

To do

☑ Confirm your processing satisfies a processing condition.
☑ Evaluate the implications of the use of that processing condition.
☑ Ensure that your use of sensitive personal data satisfies an additional processing condition.

---

38 Foster and others v British Gas (C-188/89).
39 Foster and others v British Gas (C-188/89).
40 Article 10.
41 Article 6(1).
42 Article 6(1)(e).
43 Foster and others v British Gas (C-188/89).
44 Article 37(1)(a).
45 Article 49(3).
Consent and children

Under the GDPR, it will become much more difficult to obtain a valid consent.

The GDPR imposes onerous requirements on consent (see Consent - Mission Impossible) and seeking consent will only be appropriate if the individual has a genuine choice over the matter, for example, whether to be sent marketing materials.

In other cases, you should rely on an alternative processing condition, such as the legitimate interest condition (see Processing conditions).

If you do decide to rely on consent, you should review the way you obtain consent to confirm it meets the requirements of the GDPR. For example, ensuring that you are not using pre-ticked boxes and the request for consent is separate from other matters.

Key points

> Obtaining consent from an individual is just one way to justify processing their personal data. There are other justifications.

> It will be much harder for you to obtain a valid consent under the GDPR. Individuals can also withdraw their consent at any time.

> Consent to process special category personal data and to transfer personal data outside the EU must now also be explicit.

> Consent from a child in relation to online services will only be valid if authorised by a parent. A child is someone under 16 years old, although Member States can reduce this age to 13 years old.

> There are other protections for children, including limiting the situations in which the legitimate interests condition applies and providing them with a stronger "right to be forgotten".

FAQ

Do I have to get consent from an individual?

No. Consent is only one of a number of justifications for processing the individual’s personal data. Other justifications, such as the so-called legitimate interests condition, are available. In practice, consent is only likely to be useful if the processing is optional - eg you can easily not process that personal data if the individual does not provide consent or subsequently withdraws their consent.

Consent - Mission Impossible?

Consent is a freely given, specific, informed and unambiguous indication of the individual’s wishes. The controller must keep records so it can demonstrate that consent has been given by the relevant individual. In addition:

> Plain language - A request for consent must be in an intelligible and accessible form in clear and plain language and in accordance with the Directive on unfair terms in consumer contracts.

> Separate - where the request for consent is part of a written form, it must be clearly distinguishable from other matters.

> Affirmative action - The consent must consist of a clear affirmative action. Inactivity or silence is not enough and the use of “pre-ticked boxes” is not permitted. However, consent through a course of conduct remains valid.

> No detriment - Consent will not be valid if the individual does not have a genuine free choice or if there is a detriment if they refuse or withdraw consent.

> No power imbalance - Consent might not be valid if there is a clear imbalance of power between the individual and the controller, particularly where the controller is a public authority.

> Consent to all purposes – If the relevant processing has multiple purposes, consent should be given for all of them. The meaning of this provision is not clear but it appears to be related to the concept of granularity (see below).

> Granularity - You cannot “bundle consent”. Where different processing activities are taking place, consent is presumed not valid unless the individual can consent to them separately.

> Not tied to contract - Consent is presumed not valid if it is a condition of performance of a contract.

> Withdrawable - The individual can withdraw consent at any time and must be told of that right prior to giving consent. It should be as easy to withdraw consent as it is to give it.

Finally, consent must be explicit if you are processing special category personal data or transferring personal data outside the EU. This entails a degree of formality, for example the individual ticking a box containing the express word “consent”. Explicit consent cannot be obtained through a course of conduct.
You will also need a process to manage requests to withdraw consent. In particular, what channels will you make available for a withdrawal of consent? How will you record and act on that withdrawal? If consent is withdrawn, are there any other conditions you can rely on?

Grandfathering consent
Where consent was given under the Data Protection Directive, it will continue to be valid under the GDPR if it also meets the requirements of the GDPR. This may be difficult given the new and stringent requirements for consent.

Consent and marketing
The ePrivacy Directive imposes additional constraints if you market by telephone, email or fax. For example, you can only send direct marketing to someone by email if:

> they have given you consent; or
> you have an existing relationship with them and fall within the so-called similar products and services exemption.

The ePrivacy Directive defines consent by reference to the Data Protection Directive. This will automatically be superseded by a reference to the GDPR from May 2018 onwards. In other words, obtaining consent to market by email will become a whole lot harder as well.

It is possible that more supervisory authorities will advocate the German “double opt-in” model as a requirement to prove consent has really been given by the relevant individual. This requires an email to be sent to the individual after they have provided an initial consent with a link to click on to validate that consent.

Evidence
Where you rely on consent, the burden of proof is on you to demonstrate how that consent was obtained. This means you should keep details of:

> Who consented - This should record the name or identifier for the individual.
> When they consented - This might be a copy of a dated document or online records that include a timestamp.
> What they were told at the time - This might include a master copy of the document or data capture form containing the relevant consent statement (including version numbers and dates).
> How they consent - For written consent, there should be a copy of the relevant document or form. If consent was given online, the records should include the data submitted as well as a timestamp to link it to the relevant version of the data capture form.
> Whether the individual withdrew consent - If so, when.

FAQ
What happens if someone withdraws consent?
It is likely you will have to stop processing that individual's personal data, although in some cases you may be able to rely on an alternative processing condition. Withdrawal of consent may also give the individual the right to be forgotten, ie have their data erased (see Individuals’ rights). However, withdrawal of consent does not affect the lawfulness of any processing that takes place prior to that withdrawal.

EU guidance

46 Article 7 and recitals 32, 42 and 43.
47 Recital 171.
49 Article 94(2).
50 Though interestingly, Article 95 states that the GDPR shall not impose any “additional” obligations in connection with the provision of public electronic communication services in addition to those in the ePrivacy Directive. However, firstly the marketing restrictions do not relate to the provision of public electronic services and secondly do not create a new obligation. Instead, they just amend an existing obligation.
Additional protection for children

The GDPR contains specific protections for children. You can only get consent from a child in relation to online services if it is authorised by a parent. A child is someone below the age of 16, though Member States can reduce this age to 13.\(^{51}\)

See National laws and regulators for details of the age at which a child can provide consent in each Member State.

The GDPR does not prevent you from relying on alternative processing conditions, though it may be difficult. In particular, it will be hard to fall within the legitimate interests condition when dealing with a child.\(^{52}\) The GDPR expressly states that consent is not necessary when providing preventive or counselling services to a child.\(^{53}\)

The GDPR does not apply this restriction when obtaining consent from a child offline but, given the tight controls on consent, you may still wish to obtain parental authorisation.

The GDPR contains some other miscellaneous provisions affecting children. In particular:

> your privacy policies must be very clear and simple if they are aimed at children;\(^{54}\)

> importantly, profiling and automated decision making should not be applied to children;\(^{55}\) and

> the right to be forgotten applies very strongly to children.\(^{56}\)

You should also consider whether there are additional national laws in Member States that affect the processing of personal data about children.

Not all consents are created equal - Bank secrecy

The need for consent doesn’t just arise under data protection laws but also in a number of other areas of law. For example, if you are subject to bank secrecy laws, it is very likely you will need consent to disclose customer information as these laws do not have a wide range of alternative conditions to fall back on (e.g. most bank secrecy laws do not have an equivalent to the legitimate interests condition to justify disclosure in the absence of consent).

This raises some interesting possibilities. You may find that you ask for, and obtain, a valid consent for the purposes of bank secrecy laws, but that consent is not valid for data protection purposes (e.g. because it is tied to performance of the banking contract or is withdrawn).

Given you must make it clear which processing condition you are relying on (see Why processing conditions matter), this could lead to some curious privacy notices. For example having to tell your customers they “consent” to certain disclosures under banking secrecy laws but only “acknowledge” their personal data will be processed under the GDPR, for which a different processing condition will apply.

To do

- Review your processes to obtain consent to ensure those consents are valid.
- If you can rely on an alternative basis for processing, especially in light of the right to withdraw consent.
- If you do rely on consent, put in place processes to record and act on a withdrawal of consent.

---

51 Article 8.
52 Article 6(1)(f).
53 Recital 38.
54 Recital 58.
55 Recital 71.
56 Recital 65.
One of the key aims of the GDPR is to empower individuals and give them control over their personal data. Empowerment was to be delivered through a swathe of new rights, led by a new “right to be forgotten” and “right to portability”. In practice, turning a catchy headline into workable rights has proved challenging.

Framework
These rights apply when you process personal data as controller. The rights all operate under broadly the same framework:

> Free. Individuals can exercise these rights for free.
> Time. You must comply within a month. If the request is complex or the individual makes a number of requests, you can extend this by two months.
> Excessive. Where the request is manifestly unfounded or excessive can you charge a fee or refuse the request. You have the burden of proving this is the case.
> Verification. You should verify the identity of the individual making the request. You can ask the individual for additional information to verify their identity.

New rights – Right “to be forgotten”, restrict processing and to object
These three rights are both complicated and closely interlinked. The flowchart overleaf sets out how these rights work.

If you operate a consumer-facing business, you should think about how they affect your business and how you will deal with them, including template responses and system changes.

It is also likely that many individuals will make a “combination request”, simultaneously asking the controller for copies of their personal data, to stop processing the personal data and to erase the personal data.

These combination requests will inevitably be more difficult to handle.

New rights – Data portability
Individuals have a right to access their personal data through a subject access request (see opposite). The data portability enhances this right, giving the individual the right to get that personal data in a machine readable format. Individuals can also ask for the data to be transferred directly from one controller to another.

In practice, this will be a useful right for individuals in limited situations, such as transferring between social networks or other services.

FAQ
A customer has asked to be “forgotten” and for all his data to be deleted. Do I have to comply?
It depends. Assuming the customer is an individual, they do have a right to be forgotten but that right is not absolute. In particular, you would need to confirm a range of issues such as whether you were just relying on consent to process his or her data and whether you have a continuing need to hold the relevant personal data. In some cases, you may need to quarantine his or her personal data rather than delete it. The position is complex. You will need to put a process in place to manage these requests.
cloud providers. Its application in other situations is not clear.

**Existing rights – Subject access requests**

Individuals can make a subject access request to obtain copies of their personal data. The following provisions apply to such a request:

> **Free** – As set out above, you must respond to the subject access request for free. However, you can charge if the individual asks for further copies of their personal data.^60^

> **Excessive requests** - You can refuse to respond to the request if it is manifestly unfounded or excessive. The GDPR states that where large volumes of personal data are processed, the individual should specify exactly what information or processing their request relates to.^61^ However, it is not clear how far this protects the controller from unreasonable subject access requests, such as trawling emails to respond to subject access requests.

> **Electronic access** - It must be possible to make requests electronically (presumably by email). Where such a request is made, the information should also be provided electronically, unless otherwise requested by the individual. Where possible, the individual should also be able to get secure remote access to their personal data.^62^

> **Purpose of requests** - The request should allow the individual to be aware of and verify the lawfulness of the processing you are carrying out.^63^ This might allow you to push back on requests that are not made for this purpose.

> **Right to withhold** - You can withhold personal data if disclosure would “adversely affect the rights and freedoms of others”.^64^ Under the Charter of Fundamental Rights this includes a right to conduct a business. As a result, this phrase extends to protect things that might adversely affect that business and may provide a basis to withhold intellectual property rights, trade secrets and confidential information.^65^ Some Member States have also introduced further national derogations for personal data that benefits from legal privilege or that would prejudice law enforcement, regulatory or judicial functions.

**Existing rights - Profiling and automated decision making**

Individuals have the right not to be subject to decisions made automatically that produce legal effects or significantly affect the individual.^66^ However, this right does not apply where the decision is:

> based on explicit consent from the individual, subject to suitable safeguards, including a right for a human review of the decision;

> necessary for a contract with the individual, subject to suitable safeguards, including a right for a human review of the decision; or

> authorised by EU or Member State law.

Additional restrictions apply to automated decision making or profiling using sensitive personal data or carried out on children.

**Marketing**

Individuals can object to the processing of their personal data for direct marketing. These objections must be respected.

---

^57^ The right to object arose under the old Directive but is much stronger under the GDPR.

58 Article 17, 18 and 21.

59 Article 20.

60 See the Article 29 Working Party’s Guidelines on the right to data portability (WP 242 rev.01).

61 Recital 63.

62 Article 12(5).

63 Article 12(5) and recital 63.

64 Article 12(5) and recital 63.

65 Recital 63.

66 Article 22.
### Data subjects’ rights

<table>
<thead>
<tr>
<th>When does the right apply?</th>
<th>Exemptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must comply with the request where your processing is based on one of the following processing conditions:</td>
<td>You do not need to comply if the processing is:</td>
</tr>
<tr>
<td>&gt; public interest; or</td>
<td>&gt; for legal claims; or</td>
</tr>
<tr>
<td>&gt; the legitimate interest condition.</td>
<td>&gt; based on a compelling legitimate interest which override the interests of the individual.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>You must comply with the request where:</td>
<td>You do not need to comply if the processing is:</td>
</tr>
<tr>
<td>&gt; the individual has <strong>objected</strong> to the processing and (other than in relation to objections to direct marketing) there are no overriding legitimate grounds to justify that processing;</td>
<td>&gt; necessary for rights of freedom of expression or information;</td>
</tr>
<tr>
<td>&gt; the personal data is no longer needed for the purpose for which it was collected or processed;</td>
<td>&gt; for compliance with a legal obligation under EU or Member State law;</td>
</tr>
<tr>
<td>&gt; the individual withdraws consent and there are no other grounds for the processing;</td>
<td>&gt; in the public interest or carried out by an official authority;</td>
</tr>
<tr>
<td>&gt; the personal data is unlawfully processed;</td>
<td>&gt; for public interest in the area of public health;</td>
</tr>
<tr>
<td>&gt; there is a legal obligation under EU or Member State law to erase the personal data;</td>
<td>&gt; for archiving, scientific or historical research;</td>
</tr>
<tr>
<td>&gt; personal data was processed in connection with an online service offered to a child.</td>
<td>&gt; or</td>
</tr>
<tr>
<td></td>
<td>&gt; for legal claims.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>You must comply with the request where:</td>
<td>None.</td>
</tr>
<tr>
<td>&gt; the individual has <strong>objected</strong> to the processing and you are considering if there are overriding legitimate grounds that justify continued processing;</td>
<td></td>
</tr>
<tr>
<td>&gt; the processing is no longer necessary but retention is needed by the individual to deal with legal claims;</td>
<td></td>
</tr>
<tr>
<td>&gt; the processing is unlawful but the individual wants the data to be restricted not erased;</td>
<td></td>
</tr>
<tr>
<td>&gt; the accuracy of the personal data is being contested and the controller is verifying that data.</td>
<td></td>
</tr>
<tr>
<td>What must you do?</td>
<td>Commentary</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
</tr>
<tr>
<td>You must <strong>stop processing</strong> that individual’s personal data.</td>
<td>The right to object is similar to the existing right in the Data Protection Directive. However, the right is wide ranging and reverses the burden of proof so that the controller must show there are compelling legitimate grounds to continue processing the personal data (rather than the individual having to show there are compelling grounds to stop processing).</td>
</tr>
<tr>
<td>You must <strong>erase</strong> the personal data. If you have made that personal data public, you must take reasonable steps to inform other controllers of the request for erasure.</td>
<td>The concept of a “right to be forgotten” was one of the cornerstones of the EU Commission’s original proposals but converting this concept into a meaningful right for individuals has proved challenging. Part of the problem is that the right is not limited to search engines and so is much more ambitious than the “right to be delisted” from search engines established in Google Spain (C-131/12). As a result, the right is relatively complex both in respect of the situations in which it can be exercised and the exceptions to that right. For example, you do not have to erase the individual’s personal data if the processing is necessary for freedom of information or expression. This messy clash of fundamental rights is likely to need a case-by-case assessment. In practice, the right will primarily apply to inherently objectionable processing and, given the general obligation not to retain personal data longer than necessary, adds little to the law.</td>
</tr>
</tbody>
</table>
| Where data is restricted, you may only **process** personal data:  
> with consent of the data subject;  
> for legal claims;  
> for protection of the rights and freedoms of others; or  
> for reasons of important public interest. | This right is intended as a step down from the full right of erasure and allows controllers to quarantine data so it is only used for a more limited range of purposes such as handling legal claims. Controllers will need to ensure their systems are set up to identify restricted personal data and to limit access to that data. |
Privacy notices

An unresolved paradox

Privacy notices are one of the great unresolved paradoxes of data protection law. On the one hand, telling individuals what you are doing with their personal data is a fundamental principle of data protection law. If individuals do not have this information, they cannot validly consent to its use, exercise their rights or, ultimately, decide whether or not to give you their personal data.

On the other hand, (almost) no one reads privacy notices. This is hardly surprising. One academic study found it would take the average internet user 76 days to read all of the privacy notices they encounter in a year. Similarly, we conducted a study into how frequently website privacy policies are read and for how long they are read. That found only 0.2% of visitors to a website view the website's privacy policy and those that do only spend about half the time on that page needed to actually read the policy.

Many privacy policies are too long and too complex. The academic study found that the median length of the policies reviewed was approximately 2,500 words.

Approach in the GDPR

The GDPR does not resolve this tension. It requires controllers to:

> ensure their privacy notices are “concise, transparent, intelligible and easily accessible”; and

> greatly expand the information that must be included in that privacy policy (see Information you must include in your privacy notice).

In other words, privacy notices must be both shorter and longer.

Trust and layering

The solution is to think carefully about how you deliver this information to the individual. This is not just a data protection question. If you can’t tell the individual what you are going to do with their personal data in clear and simple terms, they are not likely to trust you with it. You should consider:

> Layering - Provide the individual with a short summary of the important or unusual uses of their personal data and provide a link to a full privacy policy for those who want the detail;

> Just in time - Consider using additional notices for particular interactions with the individual. For example, if signing up to a new service means their personal data will be processed for additional purposes, point this out to them.

> Plain language - Avoid jargon and legalese. The man in the street is unlikely to understand technical terms such as “personal data”, “controller” and “processor”, so use language he will understand.

> Dashboards - Consider the use of privacy dashboards to provide individuals with meaningful information about the choices they can/have made about your use of their personal data.

> Don’t be a lawyer - How about a video, cartoon or animation to explain how you intend to use the personal data? What about the use of icons?

Key points

> The GDPR increases the amount of information you need to include in your privacy notices. Those notices must also be concise and intelligible.

> The GDPR does not expressly require the use of standardised icons, but they might be introduced by the EU Commission.

FAQ

Can I use the same notice across the whole of Europe? Do I need to provide my notice in a local language?

The GDPR should standardise much of the content of your privacy notices, but it is likely that they will still need to be translated into local languages if they are directed at a consumers in a particular jurisdiction. In particular, it is hard to see how your notice can be “accessible” if it is in a language the individual does not understand. Similarly, in some Member States such as France, the use of a local language for consumers and employees is mandatory under consumer protection and employment law.

Similarly, we conducted a study into how frequently website privacy policies are read and for how long they are read. That found only 0.2% of visitors to a website view the website’s privacy policy and those that do only spend about half the time on that page needed to actually read the policy.

Many privacy policies are too long and too complex. The academic study found that the median length of the policies reviewed was approximately 2,500 words.
Practicalities and exemptions

A privacy notice must be supplied to the individual at the time they provide you with their personal data.

If you obtain that personal data from or disclose it to a third party, the notice must be provided:

> within a reasonable time after obtaining the data, but at the latest within a month;

> if the personal data is used to communicate with the individual, at the latest when that communication is made; and

> if the personal data is disclosed to a third party, at the latest when that data is disclosed.

If you obtain that personal data from a third party, there is no need to provide a privacy notice if:

> the individual already has the information;

> providing the information would be impossible or involve disproportionate effort, particularly where the processing is for archiving, scientific or historical research purposes or statistical purposes;

> the obtaining or disclosure is pursuant to EU or Member State law and there are appropriate measures to protect the individual; or

> the information is subject to professional secrecy.

Finally, if you process that personal data for a new purpose, you must give prior notification to the individual.

Icons - Not mandatory (yet)

Earlier drafts of the GDPR suggested that privacy icons would be mandatory. You would have to display a set of icons with ticks or crosses next to them to indicate if you sell personal data, use encryption, etc.

There were significant difficulties in delivering a sensible set of icons that would provide meaningful information to individuals. Therefore, the GDPR simply states that icons may be used as part of a privacy notice and enables the EU Commission to issue a delegated act setting out what the contents of those icons should be.

It appears these provisions are voluntary and there will be no obligation to use icons. However, the position is not entirely settled and supervisory authorities may make icons a de facto requirement. On that basis, this is an area to watch.

EU guidance


To do

✔ Ensure your privacy notices contain all the mandatory information disclosures.

✔ You should use the most effective way to inform individuals of your processing, such as layered or just-in-time notices.

67 The Cost of Reading Privacy Policies, Aleecia M. McDonald and Lorrie Faith Cranor, 2012.
69 Article 12(1).
70 Article 14(3).
71 Article 14(5).
72 Articles 12(7) and (8).
### Information you must include in your privacy notice

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Commentary</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Your identity, contact details and details of your representative (if any).</td>
<td>The provision of this information is straightforward.</td>
</tr>
<tr>
<td>☑ The contact details of your data protection officer.</td>
<td>The provision of this information is straightforward.</td>
</tr>
<tr>
<td>☑ The purpose and legal basis of processing. Where the legitimate interests condition is relied upon, details of those interests.</td>
<td>The need to describe the legal basis for any processing is new. It reflects the importance the GDPR places on accurately identifying the processing condition you rely on (see Why processing conditions matter).</td>
</tr>
<tr>
<td>☑ The right to withdraw consent (if this is the basis for any processing).*</td>
<td>The provision of this information is straightforward. Dealing with requests to withdraw consent may not be (see Consent and children).</td>
</tr>
<tr>
<td>☑ The categories of personal data processed.†</td>
<td>The key question is how detailed this information has to be. The guidelines suggest that the default should be to name all recipients (including processors) but, where it is fair to do so, recipients can be described in categories by indicating their type, industry, sector and sub-sector, and their location. The guidelines also suggest that, despite the reference to “general information” on sources in recital 61, individual sources should be identified. Providing this level of detail may not always be realistic.</td>
</tr>
<tr>
<td>☑ The recipients or categories of recipients of personal data.</td>
<td></td>
</tr>
<tr>
<td>☑ The source of the personal data, including use of public sources.†</td>
<td>The key question is how detailed this information has to be. The guidelines suggest vague references are not sufficient and concrete retention periods must be specified. Many businesses hold a wide variety of personal data, so it will be difficult to provide a comprehensive description in all cases. A compromise might be to include specific details of key retention periods.</td>
</tr>
<tr>
<td>☑ Details of any intended transfer outside the EU. Details of any safeguards relied upon and the means to obtain copies of transfer agreements.</td>
<td>This information is already commonly included in privacy notices. However, you will need to be more transparent about the mechanisms you are using to transfer personal data outside the EU.</td>
</tr>
<tr>
<td>☑ The period for which data will be stored or the criteria used to determine this period.*</td>
<td>The guidelines suggest vague references are not sufficient and concrete retention periods must be specified. Many businesses hold a wide variety of personal data, so it will be difficult to provide a comprehensive description in all cases. A compromise might be to include specific details of key retention periods.</td>
</tr>
<tr>
<td>☑ A list of the individual’s rights, including the right to object to direct marketing, make a subject access request, and to be “forgotten”.*</td>
<td>The provision of this information is straightforward. Dealing with individuals exercising these rights may not be (see Individuals’ rights).</td>
</tr>
<tr>
<td>☑ Details of any automated decision making, including details of the logic used and potential consequences for the individual.</td>
<td>The obligation to disclose “meaningful information about the logic used” in any automated decision making may be challenging.</td>
</tr>
<tr>
<td>☑ Whether provision of personal data is a statutory or contractual requirement, whether disclosure is mandatory and the consequence of not disclosing personal data.*‡</td>
<td>The provision of this information is straightforward.</td>
</tr>
<tr>
<td>☑ The right to complain to a supervisory authority.*</td>
<td>This should tell individuals they can complain in their place of residence or work, or the place of infringement.</td>
</tr>
</tbody>
</table>

* Arguably some of this information might only be needed to the extent necessary to ensure fair and transparent processing (see Article 13(2) and 14(2)). However, the guidelines suggest it should be included in all privacy notices.

† Only needed when personal data is obtained from a third party.

‡ Only needed when collecting personal data directly from the individual.

---

73 See the Article 29 Working Party’s Guidelines on transparency (WP 260 rev.01).
The GDPR will require you not just to comply, but to be seen to comply

New concepts, such as accountability, privacy by design and privacy impact assessments will allow supervisory authorities to intrude further into the back office of your business than under the current regime.

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 default.

Records of data processing

For businesses, one of the key selling points of the GDPR is abolishing the need to notify data processing activities to a local supervisory authority. This is a welcome change but businesses will still need to keep records of much the same information (albeit not actually file those records with the supervisory authority).

Details of these record keeping obligations are set out in the table opposite.

Various local supervisory authorities have issued templates to use to satisfy this record-keeping obligation. In some cases, the templates suggest the records must be significantly more detailed than the information previously needed to satisfy the notification obligation.

Small businesses employing fewer than 250 employees are exempt from these record keeping requirements unless their processing activities are risky, frequent or include sensitive personal data. This exemption will therefore rarely be used.

FAQ

How can I “demonstrate” I am complying with the GDPR?

You will need to update or create suitable policies that set out how you process personal data. You should also consider other compliance measures, including setting up a clear compliance structure, allocating responsibility for compliance, staff training and audit. It might also involve technical measures such as minimising processing of personal data, pseudonymisation, giving individuals greater control and visibility and applying suitable security measures.

Record keeping obligations

Controller

If you act as a controller, you must keep a record of the following information:

> your name and contact details and, where applicable, any joint controllers, representatives and data protection officers;
> the purposes of the processing;
> a description of the categories of data subjects and of the categories of personal data;
> the categories of recipients, including recipients in third countries or international organisations;
> details of transfers of personal data to third countries (where applicable);
> retention periods for different categories of personal data (where possible); and
> a general description of the security measures employed (where possible).

Processor

If you act as a data processor, you must keep the following records:

> your name and contact details and, where applicable, representatives and data protection officers;
> the name and contact details of each controller you act for including, where applicable, representatives and data protection officers;
> the categories of processing carried out on behalf of each controller;
> details of transfers of personal data to third countries (where possible);
> a general description of the security measures employed (where possible).
Privacy impact assessments

Many businesses already incorporate privacy impact assessments into their product development cycle. The GDPR will make this mandatory for any new project that is likely to create “high risks” for individuals. The process for carrying out this assessment is set out in the Privacy impact assessment flowchart overleaf. The following points are worth highlighting:

> **High Risk** - An assessment is required if the processing is likely to be “high risk”.  

> **Assessment** - Where an assessment is needed, advice must be sought from your data protection officer (if applicable). You may also have to consult with individuals.

> **Consult supervisory authority** - You must consult your supervisory authority if the assessment indicates the processing would be high risk “in the absence of measures taken by the controller to mitigate the risk”. The guidance confirms that consultation is only needed where the risks identified in relation to that project cannot be resolved by the controller – ie the project remains high risk despite the mitigating factors.

> **Timing** - The consultation with the supervisory authority may take time. The authority has up to 14 weeks to consider the application and can extend the time whilst waiting for more information. Many supervisory authorities have limited resources. If there is an influx of consultation requests, it is hard to see how they can deal with them in a timely manner or at all.

Codes & certification

The GDPR envisages co-GDPR through the development of private sector Codes of Conduct or Certification. These are heavyweight programmes that must be approved by a supervisory authority and require supervision by an independent third party.

Complying with Codes of Conduct or obtaining a Certification can, however, provide a range of benefits. For example, they can help demonstrate compliance with the GDPR by clarifying exactly what the general requirements in the GDPR mean in a particular sector or in relation to a particular type of processing (eg provide clarity on what security measures are appropriate). They can also be used to justify international transfers of personal data (see International transfers).

The use of Codes of Conduct and Certification are a welcome means to provide an industry-led approach to compliance and to reduce the burden on supervisory authorities. If a Code of Conduct or Certification is developed in your sector, you should track its progress carefully and consider becoming involved in its development. Whilst the GDPR treats both Codes of Conduct and Certification as an optional means of compliance, there is a risk they could lead to de facto requirements in your sector.

FAQ

**What policies do I need?**

It depends on your business. You would expect a large business to have a general data protection policy and policies that address the data protection issues arising out of marketing, data security, recruitment, record retention and monitoring. These do not have to be stand-alone policies and the data protection issues might be built into a wider policy.

**To do**

☑ You will have to ensure you have appropriate compliance policies backed by training and audit.

☑ You will need to maintain a record of the processing you are carrying out (unless exempt).

☑ You should ensure your development processes include a privacy impact assessment, where necessary.

EU guidance


The Article 29 Working Party’s Position Paper on the derogations from the obligation to maintain records, April 2018.

FAQ

**What policies do I need?**

It depends on your business. You would expect a large business to have a general data protection policy and policies that address the data protection issues arising out of marketing, data security, recruitment, record retention and monitoring. These do not have to be stand-alone policies and the data protection issues might be built into a wider policy.

**To do**

☑ You will have to ensure you have appropriate compliance policies backed by training and audit.

☑ You will need to maintain a record of the processing you are carrying out (unless exempt).

☑ You should ensure your development processes include a privacy impact assessment, where necessary.

---

78 Article 35(2).
79 Article 36(1).
80 See page 18 of the Article 29 Working Party’s Guidelines on data protection impact assessments (WP 248 rev.01).
81 Articles 40-43.
Privacy Impact Assessments

**A new processing activity**

*Is the processing likely to be “high risk”?* The guidelines\(^2\) suggest that a project will be high risk if it meets two or more of the following criteria:

- Evaluation or scoring of individuals
- Automated decision making with significant effects
- Systematic monitoring
- Sensitive or highly personal data
- Data processed on a large scale
- Matching or combining data
- Data about vulnerable people
- Innovative uses or technology
- May prevent individuals exercising rights or entering contracts

You must also check if your processing activities are listed in the relevant supervisory authority’s list of “high risk” processing.

\[^2\] See page 9 of the Article 29 Working Party’s Guidelines on data protection impact assessments (WP 248 rev.01).

**You must carry out an assessment.** Your data protection impact assessment must be documented and must contain the following information:

- a description of the processing, including its purposes and any legitimate interests pursued by the controller;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to individuals; and
- the measures taken to address those risks.

You must seek advice from your data protection officer (if appointed) and may have to consult with affected individuals or their representatives.

**Is the processing still “high risk”?** Does the assessment indicate your processing is high risk despite measures taken to mitigate that risk?

**You must consult your supervisory authority.** The supervisory authority will consider if your processing is compatible with the GDPR. The supervisory authority should respond within eight weeks, but can extend this period by a further six weeks if extra time is needed due to the complexity of the processing. These time periods are suspended during periods in which the supervisory authority is waiting for further information from you.

**Assessment complete**

The assessment process is complete.
Data protection officers are an important aspect of the accountability principle. They are a means to ensure compliance with GDPR without external intervention by the supervisory authority. They were an existing feature of many Member States’ data protection laws, such as German law.

Appointment and voluntary appointment

The obligation to appoint a data protection officer applies to both controllers and processors but only applies if you are a public authority or carrying out intrusive processing, see table. If you are not obliged to appoint a data protection officer, or the position is not clear, you may want to appoint one on a voluntary basis. The data protection officer can both spearhead your compliance programme and act as a point of contact with your supervisory authority. However, a voluntary appointment will bring all of the provisions of the GDPR into play (such as protection from dismissal). If you want to avoid this, you should be careful of the job title you offer and how you describe and scope this role.

Service companies

The data protection officer can either be an employee or a third party appointed on the basis of a service contract. That service provider can consist of an individual or team of individuals, so long as they are all suitably qualified. There are various service providers who offer this service.

FAQ

What qualifications does the data protection officer need?

The data protection officer must have the right professional qualities and expert knowledge of data protection law. There is no express requirement for them to hold any particular qualification or certification. However, obtaining appropriate qualifications will be an effective way to demonstrate expert knowledge (and may help them to do their job properly).

FAQ

Does a data protection officer have personal liability?

A data protection officer will not normally have personal responsibility for non-compliance with the GDPR by the relevant controller. However, personal liability might arise in individual Member States either on the basis of general national law or because of the national law implementing the GDPR. For example, under the UK Data Protection Act 2018 directors and similar officers can be personally liable for an offence committed by a body corporate if it is the result of the director and similar officer's consent, connivance or neglect. This provision potentially applies to data protection officers.
Can I dismiss someone once they become my data protection officer?

You cannot dismiss or penalise the data protection officer for performing their role. This does not seem to prevent you appointing someone for a fixed term or for the position to be terminable on notice. In particular, the earlier proposals that the data protection officer be appointed for a minimum term of four years were dropped from the GDPR.

You should also be able to dismiss the data protection officer for behaviour unconnected with their role, subject to local employment law.

Can my CIO be our data protection officer?

The data protection officer can have a part-time role but cannot have other functions that conflict with this role. This typically means, the data protection officer should not also act as chief executive, head of marketing, head of human resources, head of IT or a similar role.

The role of data protection officer

The data protection officer is responsible for monitoring compliance with the GDPR, providing information and advice, and liaising with the supervisory authority. 84 It is an important role and the data protection officer:

- must report to the highest level of management within your business;
- must be able to operate independently and not be dismissed or penalised for performing their tasks; but
- can have other roles so long as they do not give rise to a conflict of interests (ie this does not have to be a full-time role).

Larger businesses will need to consider if the data protection officer will be part of, or lead, their privacy compliance unit.

Group-wide appointment

A group of undertakings can appoint a single data protection officer. However, that data protection officer must be accessible to each undertaking and must have expert knowledge of data protection law and practice. 85

This means that if you make a group-wide appointment you need to ensure that the data protection officer either has a good understanding of local law in the jurisdictions in which you operate and can speak the local language, or is supported by a team that has these capabilities.

Separately, it is not clear if a data protection officer appointed on a group-wide basis must just report into the management of the top company within that organisation or also has to report to the highest level of management for every operating company within the group. Having multiple reporting obligations across the whole group may count against the appointment of a group wide data protection officer.

EU guidance


To do

- Ensure you have appointed a data protection officer where mandated.
- Consider if you want to appoint a single data protection officer for the whole of your business or if you want to make individual appointments for each legal entity and/or jurisdiction.

84 Articles 38-39.
85 Articles 37(2) and (3).
Data security and breach notification

Key points

> The GDPR requires you to keep personal data secure. This obligation is expressed in general terms but does indicate some enhanced measures, such as encryption, may be needed.

> Controllers must report data breaches to their supervisory authority (unless the breach is unlikely to be a risk for individuals). That notification should normally be made within 72 hours. You may also have to tell affected individuals.

Data security is a priority for all businesses

Each year there are more high-profile cyber casualties as businesses continue to struggle to protect their systems from attacks.

This focus on data security is reflected in the enhanced data security obligations in the GDPR and the parallel obligations in the Network and Information Security Directive. However, all large businesses should consider themselves a target and take steps to secure their systems regardless of these developments.

New security obligations - optional or not?

The GDPR applies the same broad security obligation as the old Data Protection Directive, requiring controllers and processors to take appropriate technical and organisational measures to protect their systems. This broad obligation is supplemented by additional obligations to take the following steps, where appropriate: 86

> the pseudonymisation and encryption of personal data;

> the ability to ensure the ongoing confidentiality, integrity, availability and resilience of its information technology systems;

> the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

> a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

These are not mandatory obligations. Instead, they only apply “where appropriate” thus indicating they may not be needed in all cases. However, regulators often approach security breaches with the benefit of hindsight. Businesses that do not implement these measures will be pushed very hard to explain why they have not done so.

FAQ

How does the breach notification obligation relate to the obligations in the Cyber Security Directive?

The obligations in the GDPR apply in parallel with those in the Network and Information Security Directive and the ePrivacy Directive. In some Member States, there may be multiple notification obligations, which may need to be made to different regulators.

Notice of breach

One of the most striking changes in the GDPR is the obligation on controllers to notify the supervisory authority and individuals of personal data breaches, in some cases. 87 The process is set out overleaf.

The introduction of this breach notification obligation was widely expected. Telecoms providers have been subject to these obligations since 2011 and breach notification is common in other jurisdictions, such as the US.

Making a notification may be the first step towards a large fine. Poor data security has been a priority for many supervisory authorities and notifying the breaches does not provide any technical immunity from sanctions (and has not prevented fines being levied in the past).

Finally, you must keep a record of all security breaches, regardless of whether they need to be notified to the supervisory authority.

EU guidance

Data security and breach notification

86 Articles 32.
87 Articles 33 and 34.

To do

Consider setting up a central breach management unit to collate, review and notify breaches, where appropriate.

Review and update your security measures in light of the increased security obligations in the GDPR.

---

When does a breach create “risks” for individuals?
Assessing whether a personal data breach creates risk, and so must be notified to the relevant supervisory authority, requires an assessment of all the relevant circumstances. They include:

- **Type.** A personal data breach can result from a loss of confidentiality, integrity or availability. A loss of confidentiality will normally be riskier.
- **Nature and volume.** The more sensitive the personal data, the greater the risk. For example, the loss of financial details could lead to identity theft.
- **Identifiable.** If the individuals are not easily identifiable, (eg pseudonymised), that is likely to reduce the risk.
- **Severity of consequences.** This partly depends on what happens to the data after the breach. If it has been accidently sent to a “trusted recipient” who confirms the data has been deleted, that will greatly reduce the risk.
- **Special characteristics.** The characteristics of the controller or individual will be relevant.
- **Number of individuals.** The greater the number of individuals affected, the greater the risk. However, a breach can be risky even if only a single individual is affected.

Centralised breach reporting units
In practice, large businesses are likely to be best served by a centralised unit to which data breaches can be reported, analysed, recorded and the right notifications made to the right regulators.

In some cases, this is potentially quite complex. You may have to make separate reports to the supervisory authority (under the GDPR), the competent authority/CSIRT (under the Network and Information Security Directive), the telecoms authority (under the ePrivacy Directive) and other sector-specific authorities (for example, the financial regulatory authority under local financial services law).

These reports might have different trigger events, need different content and be subject to different reporting deadlines. If you operate in multiple jurisdictions, you may also have to make these reports to all of the national regulators in those jurisdictions. This is only likely to be manageable if you have a team that are trained to manage the process.

---

The Network and Information Systems Directive

**When did it come into force?**

The Network and Information Systems Directive should have been implemented in each Member State by 10 May 2018. An overview of the implementation of this law in Belgium, France, Germany, Spain and the UK is available here.

**Who does it apply to?**

The national implementations of the Directive will apply to:

- operators of essential services designated by Member States. This potentially covers business in the following sectors; energy, transport, banking, financial markets infrastructure, health, water supply and digital infrastructure. It does not apply to telecoms providers who are instead subject to the security obligations in the ePrivacy and Framework Directives; and
- digital service providers. These are operators of online marketplaces, search engines and cloud computing services.

**Does it contain breach notification obligations?**
Yes. Any “incidents having a significant impact” on the relevant services must be notified to the competent regulator. Importantly, it may be a different regulator to the supervisory authority under the GDPR. In addition, the incident does not have to involve the loss of data (ie it could instead involve the failure of critical infrastructure).

**Does it contain data security obligations?**
Yes. Designated operators of essential services and digital service providers must ensure the security of their systems.

---

✔️ To do

- Consider setting up a central breach management unit to collate, review and notify breaches, where appropriate.
- Review and update your security measures in light of the increased security obligations in the GDPR.
Breach notification process

You become aware of a personal data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It arises where there is a breach of confidentiality, integrity or availability. For example, it would include a ransomware attack even if the relevant personal data is not disclosed to a third party.

Is the breach a “risk”?

You must consider if the personal data breach is likely to be a risk to individuals. The preceding page sets out when a “risk” is likely to arise.

Notification is not required

However, you must document the personal data breach.

You must tell the supervisory authority

You must notify the supervisory authority without undue delay and, where feasible, within 72 hours from when you become aware of the breach.

That notification should contain specified details of the breach. If you can’t provide all of those details immediately, you can provide them in stages.

Is the breach “high risk”?

You must consider if the breach is a high risk for individuals. See New concepts for an analysis of when a “high risk” arises.

The breach will not be high risk if the data is encrypted or other protective measures are in place.

No further notification required

The process is at an end.

You must tell the affected individuals

You must provide affected individuals with details of the personal data breach without undue delay (though there is no fixed deadline).

If telling affected individuals directly would involve disproportionate effort, you may be able to use an alternative means of public communication, eg newspaper adverts.

---

89 See page 7 of the Article 29 Working Party’s Guidelines on personal data breach notification (WP 250 rev01).
New dynamic in negotiation with processors

The GDPR applies directly to processors. This is a significant change as processors were largely exempt from GDPR under the Data Protection Directive. Details of the obligations placed on processors under the GDPR are set out in the table opposite. These obligations, together with the significant increase in sanctions under the GDPR, are likely to change the negotiating dynamic between customers and service providers.

Data protection, or at least data security, is no longer “a customer problem” and service providers will have a much greater stake in finding the right compliance solution. This in turn has led to more intense negotiations over liability for breach of data protection law, particularly whether such liability should be capped or uncapped. Some processors have also responded by asking for cross-indemnities, though such provisions are likely to be unnecessary.

Arguably, the obligation to put a proper processing contract in place falls on both controllers and processors. This joint liability may at least make the negotiation process to include these provisions more straightforward.

Over and above these new contractual terms is the need for controllers to carefully vet and select processors to ensure they can meet all of the requirements of the GDPR. This is much broader than the previous obligation under the Directive which only required controllers to confirm that their processors had adequate data security.

Providing sensitive personal data to processors

It is very common for processing arrangements to involve at least some sensitive personal data (even if only incidentally). Under the Data Protection Directive it was not clear if a controller was allowed to disclose sensitive personal data to a processor without satisfying a relevant processing condition. In many cases this would be very difficult, if not impossible. For example, it is unlikely many outsourcings would happen if they were all conditional on the relevant individuals giving explicit consent.

Some Member States, such as Germany, implemented the Data Protection Directive to treat disclosures to processors as privileged, ie no processing condition was required. There is no similar provision under the GDPR and so no clear basis for disclosures of sensitive personal data to processors. However, in practice it seems likely that these disclosures will not need separate justification.

FAQ

Do I still have to have a contract with my data processor?

Yes. In fact, you need a much longer contract with your data processor; see Mandatory obligations for data processor contracts.

Upgrade your data processing contracts

The GDPR not only retains the need for written contracts with processors, but greatly expands the obligations they must place on their processor. A list of these obligations is set out overleaf.

The GDPR also envisages that the EU Commission or supervisory authorities will issue template wording that could be used to satisfy these requirements. However, no such model wording has been produced to date.

Arguably, the obligation to put a proper processing contract in place falls on both controllers and processors. This joint liability may at least make the negotiation process to include these provisions more straightforward.

Over and above these new contractual terms is the need for controllers to carefully vet and select processors to ensure they can meet all of the requirements of the GDPR. This is much broader than the previous obligation under the Directive which only required controllers to confirm that their processors had adequate data security.

Providing sensitive personal data to processors

It is very common for processing arrangements to involve at least some sensitive personal data (even if only incidentally). Under the Data Protection Directive it was not clear if a controller was allowed to disclose sensitive personal data to a processor without satisfying a relevant processing condition. In many cases this would be very difficult, if not impossible. For example, it is unlikely many outsourcings would happen if they were all conditional on the relevant individuals giving explicit consent.

Some Member States, such as Germany, implemented the Data Protection Directive to treat disclosures to processors as privileged, ie no processing condition was required. There is no similar provision under the GDPR and so no clear basis for disclosures of sensitive personal data to processors. However, in practice it seems likely that these disclosures will not need separate justification.
Processors and transfers outside the EEA

One curious omission from the list of new processor clauses is any substantive control on transfers of personal data outside the EEA. These transfers must be part of the documented instructions from the controller, but there are no further controls. For example, there is no express requirement on the processor to get consent from the controller for transfers outside the EEA.

The rationale might be that processors are now directly liable for transfers outside the EEA (see International transfers). In other words, the controller might be able to rely on the processor to ensure the legality of these transfers.

If so, this is a welcome change for controllers and would help avoid some of the more intractable data protection problems that commonly arise on international outsourcings. However, many processors will be unhappy with the regulatory burden being transferred to them, unless they are provided with workable compliance solutions, such as processor-to-processor Model Contracts.

<table>
<thead>
<tr>
<th>Obligations placed on processors</th>
</tr>
</thead>
<tbody>
<tr>
<td>To appoint a representative if based outside the EU.</td>
</tr>
<tr>
<td>To ensure certain minimum provisions in contracts with controllers (see Mandatory obligations for data processor contracts).</td>
</tr>
<tr>
<td>Not appoint sub-processors without specific or general authorisation of the controller and to ensure there is a contract with the sub-processor containing certain minimum provisions.</td>
</tr>
<tr>
<td>Only to process personal data on the instructions of the controller unless required to process for other purposes by EU or Member State law (but not foreign law, such as US law. This will be a major headache for many foreign processors).</td>
</tr>
<tr>
<td>To keep a record of processing carried out on behalf of a controller (see Record keeping obligations).</td>
</tr>
<tr>
<td>To co-operate with the supervisory authorities.</td>
</tr>
<tr>
<td>To implement appropriate security measures (see Data security).</td>
</tr>
<tr>
<td>To notify the controller of any personal data breach without undue delay.</td>
</tr>
<tr>
<td>To appoint a data protection officer in certain cases (see Data protection officers).</td>
</tr>
<tr>
<td>To comply with the rules on transfers of personal data outside the EEA (see International transfers).</td>
</tr>
</tbody>
</table>

✔️ To do

- If you act as controller, ensure your contract templates include this processor language. Consider if you need to update the contracts with your existing suppliers.
- If you act as processor, consider the implications of becoming directly subject to the GDPR. What liability can and should you bear? What should properly be passed back to clients and customers? Do your terms of business need to change?
- If you have historically considered yourself to be a processor to avoid being directly subject to data protection laws, consider revisiting that conclusion. Might you be better off as a controller?
## Mandatory obligations for data processor contracts

<table>
<thead>
<tr>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ The contract must contain a description of:</td>
</tr>
<tr>
<td>✓ scope, nature and purpose of the processing</td>
</tr>
<tr>
<td>✓ duration of the processing; and</td>
</tr>
<tr>
<td>✓ types of personal data and categories of data subjects.</td>
</tr>
<tr>
<td>Art. 28(3)</td>
</tr>
<tr>
<td>✓ The processor may only process personal data on the documented instructions of the controller, including as regards international transfers. There is an exception for obligations under EU or Member State law, but the processor must inform the controller (unless prohibited from doing so).</td>
</tr>
<tr>
<td>Art. 28(3)(a)</td>
</tr>
<tr>
<td>Recital 81</td>
</tr>
<tr>
<td>✓ The personnel used by the processor must be subject to a duty of confidence.</td>
</tr>
<tr>
<td>Art. 28(3)(b)</td>
</tr>
<tr>
<td>✓ The processor must keep the personal data secure.</td>
</tr>
<tr>
<td>Art. 28(3)(c)</td>
</tr>
<tr>
<td>Art. 32</td>
</tr>
<tr>
<td>✓ The processor may only use a sub-processor with the consent of the controller. That consent may be specific to a particular sub-processor or general. Where the consent is general, the processor must inform the controller of changes and give them a chance to object.</td>
</tr>
<tr>
<td>Art. 28(2)</td>
</tr>
<tr>
<td>Art. 28(3)(d)</td>
</tr>
<tr>
<td>✓ The processor must ensure it flows down these obligations to any sub-processor. The processor remains responsible for any processing by the sub-processor.</td>
</tr>
<tr>
<td>Art. 28(4)</td>
</tr>
<tr>
<td>✓ The processor must assist the controller to comply with requests from individuals exercising their rights to access, rectify, erase or object to the processing of their personal data.</td>
</tr>
<tr>
<td>Art. 28(3)(e)</td>
</tr>
<tr>
<td>✓ The processor must assist the controller with their security and data breach obligations, including notifying the controller of any personal data breach.</td>
</tr>
<tr>
<td>Art. 28(3)(f)</td>
</tr>
<tr>
<td>Art. 33(2)</td>
</tr>
<tr>
<td>✓ The processor must assist the controller should the controller need to carry out a privacy impact assessment.</td>
</tr>
<tr>
<td>Art. 28(3)(f)</td>
</tr>
<tr>
<td>✓ The processor must return or delete personal data at the end of the agreement, save to the extent the processor must keep a copy of the personal data under EU or Member State law.</td>
</tr>
<tr>
<td>Art. 28(3)(g)</td>
</tr>
<tr>
<td>✓ The processor must demonstrate its compliance with these obligations and submit to audits by the controller (or by a third party mandated by the controller). Some processors will want to agree a “mandated” third party auditor to allow their existing process of independent third party certification to continue.</td>
</tr>
<tr>
<td>Art. 28(3)(h)</td>
</tr>
<tr>
<td>✓ The processor must inform the controller if, in its opinion, the controller’s instructions would breach EU or Member State data protection law.</td>
</tr>
<tr>
<td>Art. 28(3)</td>
</tr>
</tbody>
</table>
International transfers

The restrictions on transfers of personal data are one of the more difficult aspects of European data protection laws.

The growth of the internet and the seamless transfer of personal data across national boundaries presents significant challenges. Almost no organisation fully complies with these rules.

However, the GDPR does not make radical changes, such as introducing a more flexible general accountability obligation. Instead, it largely preserves the current rules by prohibiting transfers of personal data unless certain conditions are met (see Justifications for transfers outside the EEA). Having said that, there are some relatively significant changes to these conditions. In particular,

- **Consent** - It will be hard to rely on consent from the individual as that consent must be explicit and is subject to the other limitations set out in the GDPR (see Consent and children).
- **Model Contracts** - In a welcome development, these no longer need "authorisation" from supervisory authorities. However, it is possible that some supervisory authorities will still want to be notified about their use.
- **Binding corporate rules** - Another welcome development is to put binding corporate rules on a statutory footing. Previously, they were just a soft law construct arising out of guidance from national regulators.
- **Codes of Conduct or Certification** - These provide a new justification for transfers.
- **Minor transfers** - There is a new, narrow minor transfer exemption, discussed below.

As an additional protection, transfers of personal data to a third country can be blocked for important reasons of public interest under EU or Member State law. This does not include transfers to adequate jurisdictions, but does include transfers made on another basis, for example Model Contracts. 92

Onward transfers

Another more significant change is that the GDPR regulates not just the initial transfer to a third country but also onward transfers. Under the old Directive, this is a matter of foreign law and/or any contractual obligations placed on the importer.

The extension of these restrictions to onward transfers creates a number of new complications. For example, who is liable if an onward transfer is made in breach of the GDPR? Presumably it would have to be the initial exporter as, in most cases, the importer will not be subject to the GDPR. However, it seems unfair to impose this burden on the exporter as they may have limited control over the importer (particularly where the importer acts as controller).

The minor transfer exemption - A step in the wrong direction

The GDPR allows minor transfers of personal data outside the EEA in certain very limited situations. It is intended to legitimise one-off or occasional transfers of personal data, for example where employees take their laptop with them on holiday or email a person who happens to be outside the EEA.

In some jurisdictions, such as the UK, it replaces the "presumption of adequacy" test. This allowed controllers to review all of the circumstances surrounding the transfer and conclude that the personal data would be adequately protected, regardless of the fact that there was no formal justification for the transfer.

However, the minor transfer exemption will only very rarely apply. The criteria for the transfer are set out below and will only apply in very rare instances (for completeness it also cannot be used by public authorities). For example, it seems relatively unlikely that most businesses will want to notify their supervisory authority every time one of their employees sends an email to someone in a third country, or conduct a mass mailing to inform their customers that a member of staff is taking their laptop on holiday (don’t worry, the hard drive is encrypted!).

Key points

> The GDPR prohibits the transfer of personal data outside the EEA, unless certain conditions are met. Those conditions are broadly the same as those under the Data Protection Directive.

> Full compliance with these rules will continue to be difficult. The new minor transfers exemption is unlikely to be much benefit in practice.

> Requests from foreign regulators are likely to be particularly challenging.

FAQ

I have used Commission approved Model Contracts for years - will I have to renegotiate them?

The current Model Contracts are "grandfathered" under the GDPR until revoked or replaced. However, if you are contracting with a data processor it is not clear if the Model Contracts are sufficient to meet the new requirements in the GDPR for processor contracts. Therefore you should consider supplementing them with additional obligations to meet the requirements for processor contracts.

> Minor transfers - There is a new, narrow minor transfer exemption, discussed below.

As an additional protection, transfers of personal data to a third country can be blocked for important reasons of public interest under EU or Member State law. This does not include transfers to adequate jurisdictions, but does include transfers made on another basis, for example Model Contracts.
In practice, this is likely to remain a very difficult area of law. Some supervisory authorities may continue to exercise a degree of “Nelsonian blindness”, but you should focus on bringing your transfers into compliance wherever possible, focusing on systematic or sensitive transfers.

**Foreign regulatory and litigation disclosure**

Another persistent problem is requests for personal data from foreign regulators or as part of overseas litigation. Many controllers find themselves stuck between a rock and hard place, trying to balance their data protection obligations against the risk of severe sanctions from foreign regulators and courts.

The GDPR does little to resolve this problem and, in fact, creates further complications through the new provisions in Article 48. This states:

“Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the EU or a Member State, without prejudice to other grounds for transfer.”

The meaning of this provision is far from clear, though it appears to prevent a national court from recognising a foreign disclosure request unless it is made under an appropriate treaty.

Moreover, it is not a complete ban on transfers in response to foreign requests. For example, it should still be possible to transfer personal data where there is an important public interest or where it is to establish, exercise or defend legal claims (which includes administrative, out-of-court and regulatory procedures). 93

Whether some supervisory authorities take a more aggressive interpretation of Article 48 remains to be seen.

**Schrems**

The latest iteration of the Schrems litigation (Case C-311/18) arises from a reference by the Irish Court. The CJEU has, amongst other things, been asked to consider the validity of the Model Contracts and the Privacy Shield.

However, the Irish Supreme Court is now hearing an appeal against the Irish High Court’s decision to make a reference to the CJEU. This could result in the reference being withdrawn or amended. At the least, it will delay the process as the Supreme Court is not expected to give judgment until early 2019.

**EEA States**

The GDPR has been incorporated into the EEA Agreement and, as a result, the EEA States are not treated as third countries. In other words, the restrictions on transferring personal data out of the EU do not apply to Iceland, Liechtenstein and Norway.

---

**Requirements for the minor transfer exemption**

1. No other justification could be used
2. The transfer is not repetitive
3. Only limited data subjects are affected
4. There is a compelling interest not overridden by the individuals’ interests
5. The risks have been assessed and safeguards applied
6. Supervisory authority and data subjects informed of the transfer

---

**EU guidance**

The European Data Protection Board’s Guidelines 2/2018 on derogations of Article 49.

The Article 29 Working Party’s Adequacy Referential (WP 254 rev.01).

---

**To do**

- You should review your current transfers and consider if they are justified under the GDPR.
- You should consider implementing a “structural” transfer solution (such as binding corporate rules or an intra-group agreement) as these provide a general justification for your transfers.

---

92 Article 49(5)
93 Recital 115.
Strategies for transfers of personal data outside the EEA

Model Contracts / Intra-Group Agreements

It will be possible to transfer personal data to a person outside the EU where the importer and exporter enter into the so-called Model Contracts. It is possible to enter into multiparty Model Contracts, commonly known as intra-group agreements. The existing controller-controller and controller-processor Model Contracts will be grandfathered. The GDPR removes any need to obtain authorisation from a supervisory authority.

Pros: Model Contracts are quick to implement and involve limited formalities.

Cons: There are still no processor-processor Model Contracts, so this solution cannot be used by an EU-based processor. Model Contracts can be cumbersome for multiparty transfers unless adapted to operate as an intra-group agreement (for which authorisation might still be needed). The use of Model Contracts is likely to be challenged in the latest iteration of the Schrems litigation.

Code of Conduct / Certification

Transfers to inadequate jurisdictions are possible if the importer has signed up to suitable Codes of Conduct or obtained suitable Certification (see Accountability).

Pros: Potentially covers a wide range of transfers. Limited formalities for the EU exporter.

Cons: It may take some time before suitable Codes of Conduct/Certifications become widely adopted. Compliance with the Codes of Conduct or obtaining Certification may be time consuming and costly for the importer.

Binding corporate rules (BCRs)

BCRs are a set of binding obligations under which a group of undertakings commit to process personal data in accordance with the GDPR. BCRs will be put on a statutory footing and will be available to both controllers and processors.

Pros: BCRs will become increasingly important as a means to justify transfers of personal data outside the EU and generally demonstrating compliance with the GDPR.

Cons: Only apply within a group of undertakings so do not cover transfers made to third parties (save to the extent the transfer is to a processor operating under processor BCRs). They must also be approved by the supervisory authority, which can be a costly and time consuming process.

Privacy Shield

The Privacy Shield is the replacement to the US Safe Harbor scheme, which was struck down by the CJEU in Schrems (C-362/14). It was adopted on 12 July 2016.

Pros: Potentially covers a wide range of transfers. Limited formalities for the EU exporter.

Cons: Only covers transfers to the US. Compliance with the Privacy Shield is potentially onerous. The Privacy Shield is likely to be subject to further legal challenge in the latest iteration of the Schrems litigation.
International transfers

The GDPR introduces a new exemption for minor transfers. It is only available in limited situations; see The minor transfer exemption.

Pros:
May be helpful in limited cases.

Cons:
The minor transfer exemption will only apply in very limited situations. For example, the obligation to inform the supervisory authority and individual of the transfer means it will be impracticable in many cases.

Minor transfers

The GDPR also permits a transfer if it is:
> occasional and necessary for the performance of a contract with the individual or in the individual’s interest;
> necessary for important reasons of public interest. That public interest must be recognised under EU or Member State law;
> occasional and necessary for the establishment, exercise or defence of legal claims;
> necessary for the vital interests of an individual where the individual is unable to give consent; or
> from a public register.

Pros:
Limited formalities.

Cons:
These conditions are very fact-specific and only apply in limited circumstances.

Other derogations

It will be possible to transfer personal data to a jurisdiction that provides adequate data protection laws. Adequacy means having data protection laws that are “essentially equivalent” to those in the GDPR. The current adequacy findings will all be grandfathered in the short term, ie the following countries will continue to provide adequate protection: Andorra, Argentina, Canada (partially), Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland and Uruguay. Japan is in the process of being found adequate. The adequacy findings must be reviewed every four years.

Pros:
Transfers to adequate countries are simple and straightforward.

Cons:
Very few adequacy findings have been made.

“Whitelisted” jurisdictions

Transfers to inadequate jurisdictions are possible with the explicit consent of the individual.

Pros:
Potentially available in a range of situations. Limited formalities.

Cons:
It will become much harder to obtain a valid consent under the GDPR (see Consent and children). For example, consent may not be valid if it is tied to performance of a contract and can be withdrawn at any time. In practice, it is only likely to be useful in limited situations.
Sanctions

**Fines**
One of the aims of the GDPR was to make data protection a boardroom issue. It introduces an antitrust-type sanction regime with fines of up to 4% of annual worldwide turnover or €20m, whichever is the greater. These fines apply to breaches of many of the provisions of the GDPR, including failure to comply with the six general principles or carrying out processing without satisfying a processing condition.

A limited number of breaches fall into a lower tier and so are subject to fines of up to 2% of annual worldwide turnover or €10m, whichever is the greater. Failing to notify a personal data breach or put in place an adequate contract with a processor fall into this lower tier.

When deciding whether to impose a fine and the level of the fine, the supervisory authority must consider a wide range of factors. This includes the gravity of the breach, whether the breach was intentional or negligent, any steps to mitigate the breach, the financial benefit derived from the breach and the degree of co-operation with the supervisory authority.

Controllers and processors can appeal to the courts to challenge any fine or other sanction imposed upon them.

**Other sanctions**
Supervisory authorities will have a wide range of other powers and sanctions at their disposal. This includes investigative powers, such as the ability to demand information from controllers and processors, and to carry out audits.

They will also have corrective powers enabling them to issue warning or reprimands, to enforce an individual’s rights and to issue a temporary and permanent ban on processing.

**Claims by individuals**
Individuals will have a right to bring a claim against a controller or (importantly) processor in court. They will have the right to recover both material damage and non-material damage (eg distress). Where more than one controller and/or processor is involved, they will be jointly liable for compensation.

In certain cases, not-for-profit bodies can bring a representative action on behalf of individuals.

**What is your attitude to risk?**
The GDPR applies to any processing of personal data. In the modern world, it touches almost everything you do. This makes compliance very challenging given its flexible and principle-based approach to GDPR and the step change in sanctions.

There is a real danger this will lead, at least initially, to conservative advice, chilling innovation within your business. There are three key issues to watch out for:

- **Uncertainty** - While much of the GDPR is familiar, there are a number of new provisions and it will take time to fully understand what they mean.
- **Value judgements** - In many cases, you will need to make a subjective judgement on whether processing is

---

**Key points**

> There is a step change in sanctions. Supervisory authorities will be able to issue fines of up to 4% of annual worldwide turnover or €20 million.

> Supervisory authorities will have a wide range of other powers. They can audit you, issue warnings and issue a temporary and permanent ban on processing.

> Individuals can sue you for compensation to recover both material damage and non-material damage (eg distress).

---

**FAQ**

Is the fine of 4% of annual worldwide turnover calculated on a group-wide basis?

Yes. Administrative fines are applied to “undertakings” which are as defined by reference to the competition law definition in Articles 101 and 102 TFEU. This views undertakings as economic units, so potentially includes group companies.
Sanctions

Lawful. For example, are you pursuing a legitimate interest and does it override the interests of the individual? Is the imbalance of power between you and the individual so strong as to vitiate any consent? There is no right or wrong answer to this. You should think about how you will encourage sound decision making within your business and document your decisions appropriately.

> Technical non-compliance - In some cases, you will do things that clearly breach the GDPR. For example, if one of your employees takes a laptop on a work trip to the US, that is likely to be a breach of the rules on transborder dataflow (assuming you are not going to inform the regulator and every individual whose information is on the laptop). Similarly, if your company is involved in a business sale, that will normally involve the transfer of a whole range of books and records, including emails. There is no processing condition that will justify the transfer of all of the sensitive personal data in those books and records. None of these activities have stopped following the advent of the GDPR, so you should consider your attitude to these types of risks.

> Decision making framework - What sort of difficult issues are you likely to face in practice? Is it worth developing a policy or at least informal lines to take to manage them? Where a value judgement is needed, are your staff trained to take the right approach and what factors should they consider? How much latitude do your staff have to take these decisions? What is the process for escalating or at least discussing these issues in order to take a consistent position? Should you record and audit those decisions?

> Awareness - How will you keep track of guidance on the GDPR and enforcement action by your supervisory authority? What approach are your peers taking and to what extent should that provide a benchmark for your own compliance?

> Regulatory engagement - What sort of relationship do you have with your supervisory authority? Do you regularly discuss your approach to compliance with them and to what extent would you be prepared to take soundings from them?

Managing risk

The GDPR will place much greater focus on data protection compliance. There will be significant pressure both to provide sensible advice and avoid the risk of punitive sanctions. You should ask yourself the following questions:

> Scale of processing - How much personal data do you process and how sensitive is it? If you are a large social media site, a bank or you provide medical services, it is very likely you will hold large amounts of very private information about your customers. The supervisory authority will be very interested in your activities and you will need to invest heavily in your compliance. In contrast, if you just make industrial goods, you are unlikely to process significant amounts of personal data (other than perhaps in relation to your employees). You need to take steps to comply with the GDPR, but you are unlikely to be a priority for enforcement.

FAQ

Why can’t I do [X]? Does the GDPR really stop me doing this?

The GDPR has brought real change. There will be things you were doing that you simply cannot do under the GDPR. However, for many activities there is no clear right or wrong answer. Instead they require a subjective assessment of the principles in the GDPR. If [X] is a legitimate activity and is carried out in a sensible manner, you can probably do it, you may just need to be a bit more robust.

*X* is something perfectly reasonable and sensible that causes no real harm to any individual.

EU guidance

The Article 29 Working Party’s Guidelines on the application and setting of administrative fines (WP 250 rev.01).

To do

☞ You should review your current level of compliance and ensure it meets the level required under the GDPR.

☞ You should consider your overall attitude to risk and consider creating a risk assessment framework.

94 Article 83(5) and (6).
95 Article 83(4).
96 Article 58.
97 Article 82.
98 Articles 80.
National law and regulators

Key points

> The GDPR applies directly to all Member States.
> The GDPR is mainly enforced by national supervisory authorities.
> The European Data Protection Board will help ensure consistent application of the GDPR and has issued guidance on its interpretation.
> This should all bring greater harmonisation. However, there are a number of derogations under national law. It is also likely there will be differences in the way the GDPR is interpreted and enforced.

The General Data Protection Regulation (2016/679) heralds the biggest shake-up to Europe’s privacy laws for 20 years

The GDPR applies to all Member States as of 25 May 2018. As a Regulation, it is directly effective in all Member States without the need for further national legislation.

National law

However, Member States must still introduce implementing legislation to create a national supervisory authority to enforce the GDPR and to take advantage of the derogations available under it.

The supervisory authority must be independent of the Member State and appointed for a minimum period of four years. 99 It is possible for a Member State to establish more than one supervisory authority (as is the case in Germany).

The table opposite sets out the status of national implementing laws in each Member State.

This reflects the position at the date of this guide. Updated information is available from our Data Protected report: www.linklaters.com/en/insights/data-protected/home

Consistency mechanism (one stop shop)

The GDPR introduces the concept of the one stop shop to create a stronger digital market.

The final proposals are less ambitious than those originally proposed. A business 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). 100

However, a local supervisory authority will always have jurisdiction where processing is carried out on the basis of the legal obligation or public functions condition. 101

In addition, it can ask for control where the matter relates only to an establishment in its Member State or substantially affects individuals only in its Member State.

The lead supervisory authority can refuse that request but must co-ordinate its activities closely with concerned supervisory authorities. If the other supervisory authorities object to the approach taken by the lead authority, they can ask the Board to override that decision. 102

FAQ

My business operates across the EU. Do I still have to get advice from lots of local counsel?

It depends on what processing you are carrying out. There will still be significant national variations in some areas, which will require review by local counsel. One example is processing of information about employees as Member States can introduce additional protections for employees. There is also a significant overlap with national labour laws and there may be differences in the way the rules are interpreted and enforced, though hopefully the differences will narrow over time, and the GDPR contains a consistency mechanism to help do that.

The Board has a number of important functions, including:
> issuing guidance (see below);
> helping assess the adequacy of a third country’s data protection laws; and
> acting to ensure the consistent and correct application of the GDPR.

The Board has a number of important functions, including:
> issuing guidance (see below);
> helping assess the adequacy of a third country’s data protection laws; and
> acting to ensure the consistent and correct application of the GDPR.

The European Data Protection Board

The GDPR establishes the Board. The Board is composed of supervisory authorities and the European Data Protection Supervisory. The EU Commission can also participate but cannot vote.

FAQ

My business operates across the EU. Do I still have to get advice from lots of local counsel?

It depends on what processing you are carrying out. There will still be significant national variations in some areas, which will require review by local counsel. One example is processing of information about employees as Member States can introduce additional protections for employees. There is also a significant overlap with national labour laws and there may be differences in the way the rules are interpreted and enforced, though hopefully the differences will narrow over time, and the GDPR contains a consistency mechanism to help do that.

The Board has a number of important functions, including:
> issuing guidance (see below);
> helping assess the adequacy of a third country’s data protection laws; and
> acting to ensure the consistent and correct application of the GDPR.

The Board has a number of important functions, including:
> issuing guidance (see below);
> helping assess the adequacy of a third country’s data protection laws; and
> acting to ensure the consistent and correct application of the GDPR.
<table>
<thead>
<tr>
<th>Country</th>
<th>Status of national law</th>
<th>Supervisory Authority</th>
<th>Additional obligations to appoint DPO</th>
<th>Age for child consent online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Passed</td>
<td>Österreichische Datenschutzbehörde</td>
<td>No</td>
<td>14</td>
</tr>
<tr>
<td>Belgium</td>
<td>Passed</td>
<td>Autorité de protection des données</td>
<td>No</td>
<td>13</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>In draft</td>
<td></td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Croatia</td>
<td>Passed</td>
<td>Agencija za zaštitu osobnih podataka</td>
<td>No</td>
<td>16</td>
</tr>
<tr>
<td>Cyprus</td>
<td>Passed</td>
<td>Commissioner for the Protection of Personal Data</td>
<td>Potentially</td>
<td>14</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>In draft</td>
<td></td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Denmark</td>
<td>Passed</td>
<td>Datatilsynet</td>
<td>No</td>
<td>13</td>
</tr>
<tr>
<td>Estonia</td>
<td>In draft</td>
<td></td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Finland</td>
<td>Passed</td>
<td>Tietosuojavaltuutetun toimisto</td>
<td>No</td>
<td>13</td>
</tr>
<tr>
<td>France</td>
<td>Passed</td>
<td>Commission Nationale de l’Informatique et des Libertés (CNIL)</td>
<td>No</td>
<td>15</td>
</tr>
<tr>
<td>Germany</td>
<td>Passed</td>
<td>Various federal and regional authorities</td>
<td>Yes</td>
<td>16</td>
</tr>
<tr>
<td>Greece</td>
<td>In draft</td>
<td></td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Hungary</td>
<td>In draft</td>
<td></td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Ireland</td>
<td>Passed</td>
<td>Data Protection Commissioner</td>
<td>No</td>
<td>13</td>
</tr>
<tr>
<td>Italy</td>
<td>Passed</td>
<td>Garante per la protezione dei dati personali (Garante)</td>
<td>No</td>
<td>14</td>
</tr>
<tr>
<td>Latvia</td>
<td>Passed</td>
<td>Datu valsts inspekcija</td>
<td>No</td>
<td>13</td>
</tr>
<tr>
<td>Lithuania</td>
<td>Passed</td>
<td>Valstybin duomen apsaugos inspekcija</td>
<td>No</td>
<td>14</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Passed</td>
<td>Commission Nationale pour le Protection des Données (CNPD)</td>
<td>No</td>
<td>16</td>
</tr>
<tr>
<td>Malta</td>
<td>Passed</td>
<td>Information and Data Protection Commissioner</td>
<td>No</td>
<td>13</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Passed</td>
<td>Autoriteit Persoonsgegevens</td>
<td>No</td>
<td>16</td>
</tr>
<tr>
<td>Poland</td>
<td>Passed</td>
<td>Úrz du Ochrony Danych Osobowych (UODO)</td>
<td>No</td>
<td>16</td>
</tr>
<tr>
<td>Portugal</td>
<td>In draft</td>
<td></td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Romania</td>
<td>Passed</td>
<td>Nemzeti Adatvédelmi és Információszabadság Hatóság</td>
<td>No</td>
<td>16</td>
</tr>
<tr>
<td>Slovakia</td>
<td>Passed</td>
<td>Úrad na ochranu osobných údajov Slovenskej republiky</td>
<td>No</td>
<td>16</td>
</tr>
<tr>
<td>Slovenia</td>
<td>In draft</td>
<td></td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Spain</td>
<td>Passed</td>
<td>Agencia Española de Protección de Datos</td>
<td>Yes</td>
<td>14</td>
</tr>
<tr>
<td>Sweden</td>
<td>Passed</td>
<td>Datainspektionen</td>
<td>No</td>
<td>13</td>
</tr>
<tr>
<td>UK</td>
<td>Passed</td>
<td>Information Commissioner</td>
<td>No</td>
<td>13</td>
</tr>
</tbody>
</table>
Guidance

One important function of the Board is to issue guidance on the GDPR. The key guidance issued by the Board is set out below (see Key Guidance).

Importantly, the Board has not only issued some of its own guidance but also endorsed the guidance on the GDPR issued by its predecessor, the Article 29 Working Party. (However, earlier guidance from the Article 29 Working Party on the Data Protection Directive should now be treated with caution).

Full harmonisation still some way off

The aim of this new law was to strengthen the single market by creating a consistent data protection framework across the whole of the European Union.

The Data Protection Directive had to be implemented into national law in each Member State. Each implementation was slightly different leading to a patchwork of laws. The GDPR avoids this problem as it will be directly effective in all Member States without the need for national implementing laws.

This is a step in the right direction but significant national divergences are likely to remain. Some arise because Member States have limited rights to derogate from the GDPR, but they will also arise because many aspects of the GDPR are closely tied up with national law (see Overview of national derogations).

Different social and cultural attitudes to data protection are equally important. Many aspects of the GDPR are principle-based to cater for the wide range of processing and the likelihood of rapid technological change.

Key Guidance

<table>
<thead>
<tr>
<th>Issue</th>
<th>Guidance</th>
<th>Ref</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extra-territorial reach</td>
<td>EDPB Draft guidelines on territorial scope</td>
<td>3/2018</td>
<td>In draft</td>
</tr>
<tr>
<td>Consent &amp; children</td>
<td>A29WP Guidelines on consent</td>
<td>WP259 rev.01</td>
<td>April 2018</td>
</tr>
<tr>
<td>Individual rights</td>
<td>A29WP Guidelines on the right to data portability</td>
<td>WP242 rev.01</td>
<td>April 2018</td>
</tr>
<tr>
<td>Privacy notices</td>
<td>A29WP Guidelines on transparency</td>
<td>WP260 rev.01</td>
<td>April 2018</td>
</tr>
<tr>
<td>Accountability &amp; impact assessments</td>
<td>A29WP Guidelines on Data Protection Impact Assessment and “high risk” processing</td>
<td>WP248 rev.01</td>
<td>October 2017</td>
</tr>
<tr>
<td></td>
<td>EDPB Guidelines on certification and identifying certification criteria</td>
<td>1/2018</td>
<td>May 2018</td>
</tr>
<tr>
<td></td>
<td>A29WP Position Paper on the derogations from the obligation to maintain records</td>
<td>-</td>
<td>April 2018</td>
</tr>
<tr>
<td>Data protection officers</td>
<td>A29WP Guidelines on Data Protection Officers</td>
<td>WP243 rev.01</td>
<td>April 2017</td>
</tr>
<tr>
<td>Data security &amp; breach notification</td>
<td>A29WP Guidelines on personal data breach notification</td>
<td>WP250 rev.01</td>
<td>February 2018</td>
</tr>
<tr>
<td>International transfers</td>
<td>EDPB Guidelines on derogations of Article 49</td>
<td>2/2018</td>
<td>May 2018</td>
</tr>
<tr>
<td></td>
<td>A29WP Adequacy referential</td>
<td>WP254 rev.01</td>
<td>February 2018</td>
</tr>
<tr>
<td>Sanctions</td>
<td>Guidelines on the application and setting of administrative fines</td>
<td>WP253</td>
<td>October 2017</td>
</tr>
<tr>
<td>National law &amp; regulation</td>
<td>A29WP Guidelines for identifying a controller or processor’s lead supervisory authority</td>
<td>WP244 rev.01</td>
<td>April 2017</td>
</tr>
</tbody>
</table>

103 The Board has also endorsed five working documents from the Article 29 Working Party addressing the use of binding corporate rules.
Principle-based regulation is flexible, adaptable and hard to circumvent but also inherently uncertain. The interpretation of difficult concepts depends in part on cultural attitudes to privacy and subjective value judgements; what is regarded as “fair” in Stockholm may not also be regarded as “fair” in Madrid. Whilst the questions will be the same across the EU, the answers may not be.

Finally, differences in the resources and attitudes of supervisory authorities are likely to 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.

Other areas of law
The GDPR, and associated national law, are not the only laws you should consider as part of your compliance programme.

You should also consider the ePrivacy Directive. Amongst other things, this contains additional controls on marketing by email or telephone, and restrictions on the use of cookies. The EU is in the process of replacing this Directive with a new EU ePrivacy Regulation.

Similarly, the Network and Information Security Directive imposes obligations on some businesses to keep their systems secure and notify breaches to the relevant regulation (see Data security and breach notification).

Finally, the GDPR is accompanied by the Criminal Law Enforcement Data Protection Directive (2016/680) which applies to the processing of personal data by law enforcement authorities. This Directive should have been implemented in all Member States by 6 May 2018 but is not considered in this guide.

Overview of national derogations

Member States can pass laws to amend some of the obligations under the GDPR. The more important derogations are set out below:

> **Children** - Member States can reduce the age at which a child can provide valid consent online from 16 to 13 years old.\(^{104}\)

> **Data protection officers** - Member States can make the appointment of a data protection officer mandatory in additional situations.\(^{115}\)

> **Employment** - Members States can introduce further restrictions on the processing of employee data.\(^{116}\)

> **National security** - Member States can pass laws to limit rights under the GDPR in areas such as national security, crime and judicial proceedings.\(^{107}\)

> **Freedom of information** - Member States can amend the GDPR to reconcile data protection with freedom of information, to protect information subject to professional secrecy and to restrict the processing of national identity numbers.\(^{108}\)

> **Individual rights** – Member States can restrict individuals’ rights on public interest grounds.\(^{109}\)

Moreover, a large number of processing activities are dependent on national law in Member States. For example:

> **Processing conditions** - One justification for processing personal data is where it is in compliance with an obligation under EU or Member State law.\(^{110}\)

> **Criminal offences** - The processing of information about criminal offences is only permitted where authorised by EU or Member State law (or under the control of an official authority).\(^{111}\)

> **Right to be forgotten** - The right to be forgotten does not apply if the processing is necessary for compliance with a legal obligation under EU or Member State law.\(^{112}\)

> **International transfers** - A public interest recognised under Member State law may provide a basis to transfer personal data outside the EU. Equally, Member States can introduce additional restrictions on transfers.\(^{113}\)

These national derogations and the interaction with other Member States laws means the effect of the GDPR will not be fully harmonised across the EU.

---

104 Article 8.
105 Article 37(4).
106 Article 88.
107 Article 23.
108 Articles 85-91.
109 Article 23.
110 Article 61(1)(c).
111 Article 10.
112 Article 17.
113 Articles 49(4) and (5).
Brexit

The UK will leave the EU in March 2019. The conditions under which this will happen are not certain at the date of this guide. However, the UK Government remains confident it will be under the terms of a withdrawal agreement which will include a transitional period preserving the current data protection framework until December 2020.

Brexit raises the following issues:

> **UK data protection laws.** Regardless of Brexit, the UK is very likely to continue to apply the GDPR. Once the UK leaves, the Government has indicated the GDPR will be incorporated into UK law by virtue of the European Union (Withdrawal) Act 2018.

> **Transfers to the EU.** The UK Government has stated it will not impose restrictions on transfers of personal data to the EU.\(^{114}\)

> **Transfers to the UK.** Dealing with transfers of personal data from the EU to the UK is more complex given the UK will become a third country. It is hoped that the UK’s data protection laws will be found adequate by the EU Commission and thus the UK will be a “whitelisted” jurisdiction. Failing that it may be necessary to put Model Contracts in place to address such transfers.

> **Ongoing co-operation.** The UK has proposed an “adequacy +” arrangement under which the UK Information Commissioner continues to play a part in the one-stop-shop and the Board. Although there are obvious benefits to this approach for both the EU and the UK, it is not clear if this proposal will be accepted.

---

EEA States

In July 2018, the EEA Joint Committee agreed to incorporate the GDPR into the EEA Agreement. This means that Iceland, Liechtenstein and Norway must apply the GDPR. In addition, their supervisory authorities will be part of the one-stop-shop and will join the Board. However, their supervisory authorities will not have voting rights.

---

To do

- Keep track of guidance issued by supervisory authorities and the European Data Protection Board.
- Keep track of Member State laws that vary or modify the obligations in the GDPR.
- Work out where your main establishment is and who your lead supervisory authority will be.

---

\(^{114}\) In practice, any such restriction is likely prohibited by the amended Convention 108.
Summary

Extra-territorial reach
> The GDPR primarily applies to businesses established in the EU.
> Businesses based outside the EU will be caught by the GDPR if their operations are “inextricably linked” to an establishment in the EU.
> It will also apply to businesses based outside the EU that offer goods and services to, or monitor individuals in, the EU.
> These businesses will need to appoint a representative in the EU, subject to certain limited exemptions. The representative may have to accept some liability for breaches of the GDPR.

Children
> Consent from a child in relation to online services will only be valid if authorised by a parent. A child is someone under 16 years old, though Member States can reduce this age to 13 years old.
> There are other protections for children, including limiting the situations in which the legitimate interests condition applies and providing them with a stronger “right to be forgotten”.

Core rules and processing conditions
> The GDPR retains the same core rules as the Data Protection Directive and continues to regulate the processing of personal data.
> Those processing personal data do so as a controller or a processor. A processor just acts on the instructions of the controller.
> Controllers must comply with six general principles and must satisfy a processing condition. These principles and processing conditions are similar to those in the Data Protection Directive, but there are some significant changes.
> The concept of special category personal data has been retained and expanded to include genetic and biometric data.

Consent
> Obtaining consent from an individual is just one way to justify processing their personal data. There are other Justifications.
> It will be much harder for you to obtain a valid consent under the GDPR. Individuals can also withdraw their consent at any time.
> Consent to process special category personal data must be explicit. Consent to transfer personal data outside the EU must now also be explicit.

Individuals’ rights
> The GDPR largely preserves the existing rights of individuals to access their own personal data, rectify inaccurate data and challenge automated decisions about them. The GDPR also retains the right to object to direct marketing.
> There are also potentially significant new rights for individuals, including the “right to be forgotten” and the right to data portability.

Privacy notices
> The GDPR increases the amount of information you need to include in your privacy notices. Those notices must also be concise and intelligible.
> The GDPR does not expressly require the use of standardised icons, but they might be introduced by the EU Commission.

Accountability and impact assessments
> Under the GDPR, you must not only comply with the six general processing principles, but also be able to demonstrate you comply with them.
> If you are carrying out “high risk” processing, you must carry out a privacy impact assessment and, in some cases, consult your supervisory authority. This could have significant timing implications for your project.
> It may be possible to demonstrate compliance, and comply with other obligations in the GDPR, by signing up to a code of practice or becoming certified.
Summary

Data protection officer

> You may be obliged to appoint a data protection officer. This depends on what processing you carry out.

> The data protection officer must be involved in all data protection issues and cannot be dismissed or penalised for performing their role.

> The data protection officer must report directly to the highest level of management within your organisation.

Data security and breach notification

> The GDPR requires you to keep personal data secure. This obligation is expressed in general terms but does indicate that some enhanced measures, such as encryption, may be needed.

> Controllers must report data breaches to their supervisory authority (unless the breach is unlikely to be a risk for individuals). That notification should normally be made within 72 hours. You may also have to tell affected individuals.

International transfers

> The GDPR prohibits the transfer of personal data outside the EEA, unless certain conditions are met.

> Full compliance with these rules will continue to be difficult. The new minor transfers exemption is unlikely to be much benefit in practice.

> Requests from foreign regulators are likely to be particularly challenging. You may continue to be stuck between a rock and a hard place.

Sanctions

> There is a step change in sanctions. Supervisory authorities will be able to issue fines of up to 4% of annual worldwide turnover or €20 million.

> Supervisory authorities have a wide range of other powers. They can audit you, issue warnings and issue a temporary and permanent ban on processing.

> Individuals can sue you for compensation to recover both material damage and non-material damage (eg distress).

Processors

> The GDPR expands the list of provisions that controllers must include in their contracts with processors.

> Some aspects of the GDPR are directly applicable to processors. This will be a major change for some suppliers who have avoided direct regulation under the Data Protection Directive.

> Processors will be jointly and severally liable with the relevant controller for compensation claims by individuals.
Glossary

**A29WP or Article 29 Working Party** means the representative body for national regulators under the old Data Protection Directive. It has now been replaced by the Board.

**Board** means the European Data Protection Board (see *European Data Protection Board*).

**Controller** means the person who, alone or jointly, determines the purpose and means of the processing of personal data (see *Core rules and key concepts*).

**Data Protection Directive** means the old Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.


**General processing principles** means the six general principles relating to the processing of personal data set out in Article 5 of the GDPR (see *Core rules and key concepts*).

**Individual or data subject** means the living individual to whom the personal data relates (see *Core rules and key concepts*).

**Lead supervisory authority** means the supervisory authority with primary competence over a business carrying out cross border processing (see *Consistency mechanism*).

**Legitimate interests condition** means the processing condition set out in Article 6(1)(f) of the GDPR (see *Processing conditions*).

**Member State** means a member of the European Union.

**Minor transfers exemption** means the exemption in Article 49 for minor transfers (see *The minor transfer exemption - A step in the wrong direction?*).

**Model Contracts** means a form of contract approved by the EU Commission to allow the transfer of personal data to third countries. These are also known as Standard Contractual Clauses.

**Network and Information Systems Directive** means Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the EU (see *Data security and breach notification*).

**Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (see *Data security and breach notification*).

**Personal data** means information relating to an identified or identifiable living individual (see *Key concepts*).

**Privacy impact assessment** means the assessment of certain new projects for their privacy implications (see *Privacy impact assessment*).

**Processing condition** means the processing conditions set out in Article 6 of the GDPR (see *Processing conditions*).

**Processor** means a person who processes personal data on behalf of a controller (see *Key concepts*).

**Processor contract** means the contract a controller must put in place with a data processor (see *Processors*).

**Pseudonymisation** means the processing of personal data so it can no longer be attributed to an individual without the use of additional information that is kept separate and secure (see *Pseudonymised data and other risk based concepts*).

**Sensitive personal data** means special category personal data and information about criminal convictions and offences.

**Special category personal data** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation (see *Key concepts*).

**Supervisory authority** means a data protection regulator set up in a Member State (see *National laws and regulators*).
Contacts

Brussels

Tanguy Van Overstraeten
Tel: +32 2 501 94 05
tanguy.van_overstraeten@linklaters.com

Frankfurt

Daniel Pauly
Tel: +49 69 710 03 570
daniel.pauly@linklaters.com

Hong Kong

Samantha Cornelius
Tel: +852 2901 5542
samantha.cornelius@linklaters.com

Lisbon

Carlos Pinto Correia
Tel: +351 21 864 00 15
carlos.correia@linklaters.com

London

Richard Cumbley
Tel: +44 20 7456 4681
richard.cumbley@linklaters.com

Luxembourg

Yuri Auffinger
Tel: +352 26 08 83 81
yuri.auffinger@linklaters.com

Madrid

Carmen Burgos
Tel: +34 91 399 6088
carmen.burgos@linklaters.com

Moscow

Evgeny Ulumdzhiev
Tel: +7 495 797 9797
evgeny.ulumdzhiev@linklaters.com

Munich

Konrad Berger
Tel: +49 89 418 08 168
konrad.berger@linklaters.com

Paris

Sonia Cissé
Tel: +33 1 56 43 57 29
sonia.cisse@linklaters.com

Singapore

Adrian Fisher
Tel: +65 6692 5856
adrian.fisher@linklaters.com

Stockholm

Elisabet Lundgren
Tel: +46 8 665 67 77
elisabet.lundgren@linklaters.com

Tokyo

Mamiko Nagai
Tel: +81 3 6212 1232
mamiko.nagai@linklaters.com

Warsaw

Agnieszka Mencel
Tel: +48 22 526 5045
agnieszka.mencel@linklaters.com