

# Linklaters

The General Data Protection Regulation

A survival guide





# Use the opportunity

The General Data Protection Regulation promises the biggest shake up to European privacy laws for 20 years. It will apply in all Member States from 25 May 2018.

The changes needed to comply with the Regulation are significant and the two year implementation period is likely to go quickly. You should start to prepare for them now.

It is likely you will need a compliance programme to manage these changes, but don't just focus on the narrow requirements of the Regulation. Use this as an opportunity to improve the way you handle personal information. In other words, look up from the maze of articles and recitals and think about your customers, employees and other individuals. They will expect a lot more of you in a post-Regulation world.

Much of the attention has been focused on the new antitrust-type sanction regime. The threat of fines of up to 4% of annual worldwide turnover or €20million means data protection will need to be taken more seriously. There is a risk of taking this too far and chilling innovation. Those advising on the Regulation will be under significant pressure to both provide sensible advice and avoid the risk of punitive sanctions. In the short term, privacy advice is going to need a little more thought, a good deal of pragmatism and a pinch of courage.

This guide sets out the key changes under the Regulation, as well as providing a "to do" list and answers to many of the questions we have received from our clients about it.

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](mailto:tanguy.van_overstraeten@linklaters.com)



**Richard Cumbley**

Global Head of TMT/IP

Tel: (+44) 20 7456 4681

[richard.cumbley@linklaters.com](mailto:richard.cumbley@linklaters.com)



**Daniel Pauly**

Partner

Tel: (+49) 69 710 03 570

[daniel.pauly@linklaters.com](mailto:daniel.pauly@linklaters.com)



---

# Contents

Use the opportunity	3
Contents	5
The Regulation at a glance	6
Countdown to 2018	8
Extra-territorial reach	12
Core rules remain the same	15
Consent and children	22
Data subjects' rights	26
Privacy notices	30
Accountability	33
Data protection officer	36
Data security	38
Processors	42
Transfers outside the Union	46
Sanctions	50
To do	52
Glossary	53
Contacts	54

# The Regulation at a glance

## Countdown to 2018

- > The Regulation will apply in all Member States from 25 May 2018.
- > Use of a Regulation should bring greater harmonisation. However, there are a large number of national derogations. It is also likely there will be differences in the way the Regulation is interpreted and enforced in different Member States.
- > Businesses that carry out cross-border processing should be primarily regulated by the supervisory authority in the jurisdiction in which they have their main establishment.

## Extra-territorial reach

- > The Regulation primarily applies to businesses established in the Union.
- > It will also apply to businesses based outside the Union that offer goods and services to, or monitor individuals in, the Union.
- > These businesses will need to appoint a representative in the Union, subject to certain limited exemptions. The representative may have to accept liability for breaches of the Regulation.

## 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 remain the same

- > The Regulation 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.
- > All processing 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 sensitive personal data has been retained and expanded to include genetic and biometric data. It will also become much harder to process information about criminal offences in some Member States.

## 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 Regulation. Individuals can also withdraw their consent at any time.
- > As under the Data Protection Directive, consent to process sensitive personal data must be explicit. Consent to transfer personal data outside the Union must now also be explicit.

## Data subjects' rights

- > The Regulation largely preserves the existing rights of individuals to access their own personal data, rectify inaccurate data and challenge automated decisions about them. The Regulation 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. The new rights are complex and it is not clear how they will operate in practice.

## Privacy notices

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

## Accountability

- > Under the Regulation, you must not only comply with the six general 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 Regulation, by signing up to a code of practice or becoming certified.

### 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

- > The Regulation 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.

### Processors

- > The Regulation expands the list of provisions that controllers must include in their contracts with processors.
- > Some aspects of the Regulation are directly applicable to processors. This will be a major change for some suppliers who have avoided direct regulation under the Data Protection Directive by setting themselves up as processors.
- > Processors will be jointly and severally liable with the relevant controller for compensation claims by individuals.

### Transfers outside the Union

- > The Regulation prohibits the transfer of personal data outside the Union, 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. 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 (e.g. distress).

“

The Regulation promises the biggest shake-up to European privacy laws for 20 years. The changes needed to comply with the Regulation are significant and the two-year implementation period is likely to go quickly. You should start to prepare for them now.

”

# Countdown to 2018

## ! Key points

- > The Regulation will apply in all Member States from 25 May 2018.
- > Use of a Regulation should bring greater harmonisation. However, there are a large number of national derogations. It is also likely there will be differences in the way the Regulation is interpreted and enforced in different Member States.
- > Businesses that carry out cross-border processing should be primarily regulated by the supervisory authority in the jurisdiction in which it has its main establishment. However, there are exceptions to this rule.

## ? FAQ

### My business operates across the Union. 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 Regulation contains a consistency mechanism to help do that.

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

It was published in the Official Journal on 4 May 2016 and came into force on 25 May 2016. The substantive provisions will apply in all Member States from 25 May 2018.<sup>1</sup>

As a Regulation, it is directly effective in all Member States without the need for further national legislation. However, Member States will have to introduce some implementing legislation to create a national regulator and to take advantage of some of the derogations available under the Regulation (see *Overview of national derogations*).

The Regulation 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 must be implemented in all Member States by 6 May 2018 but is not considered further in this note.

### National regulators

There will be a regulator in every Member State, known as a supervisory authority. The **supervisory authority** must be independent of the Member State and appointed for a minimum period of four years.<sup>2</sup> It is possible for a Member State to establish more than one supervisory authority (as is the case today in Germany).

There will also be a European Data Protection Board (the **Board**), made up of one representative from the supervisory authorities from each Member State.<sup>3</sup> The Board will take over from the current representative body, the Article 29 Working Party, but will have a much stronger role in providing guidance and co-ordinating enforcement of the Regulation through a consistency mechanism.

### Consistency mechanism (one stop shop)

The initial proposal was for a one stop shop regulatory mechanism under which

businesses would only have to deal with a single supervisory authority for all processing carried out in the Union. However, the proposal met with significant resistance from some Member States, partly because of practical complications such as the ability of supervisory authorities to handle complaints in other languages and to manage the interaction with local law. Some Member States were also concerned that some smaller supervisory authorities would not adequately regulate larger companies that have chosen to establish themselves in that jurisdiction.

As a result, these proposals have been watered down. 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**).<sup>4</sup>

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.<sup>5</sup> 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.<sup>6</sup>

### Full harmonisation still some way off

Another aim of the Commission's proposed reforms 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. In contrast, the Regulation 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 Regulation, but they will also arise because many aspects of the Regulation 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 Regulation are principle-based to cater for the wide range of processing and the likelihood of rapid technological change. 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 Union, 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.

## ? FAQ

### How do I nominate a regulator to be my lead supervisory authority?

There is no formal nomination process but the identity of the lead supervisory authority will be obvious in many cases. In borderline cases, there may be some value in discussing the matter with the relevant supervisory authorities. Some organisations may already have a lead supervising authority in practice, for example as part of a binding corporate rules application.

## Overview of national derogations

### Member States can pass laws to amend some of the obligations under the Regulation. 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.<sup>7</sup>
- > *Data protection officers* - Member States can make the appointment of a data protection officer mandatory.<sup>8</sup>
- > *Employment* - Member States can introduce further restrictions on the processing of employee data.<sup>9</sup>
- > *National security* - Member States can pass laws to limit rights under the Regulation in areas such as national security, crime and judicial proceedings.<sup>10</sup>
- > *Freedom of information* - Member States can amend the Regulation to reconcile data protection with freedom of information, to protect information subject to professional secrecy and to restrict the processing of national identity numbers.<sup>11</sup>

### 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 Union or Member State law.<sup>12</sup>
- > *Criminal offences* - The processing of information about criminal offences is only permitted where authorised by Union or Member State law (or under the control of an official authority).<sup>13</sup>
- > *Right to be forgotten* - The right to be forgotten does not apply if the processing is necessary for compliance with a legal obligation under Union or Member State law.<sup>14</sup>
- > *International transfers* - A public interest recognised under Member State law may provide a basis to transfer personal data outside of the Union. Equally, Member States can introduce additional restrictions on transfers.<sup>15</sup>

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

1 Article 99(2).

2 Articles 51-54.

3 Articles 68-79.

4 Article 56.

5 Article 55(2).

6 Articles 56 and 60.

7 Article 8.

8 Article 37(4).

9 Article 88.

10 Article 23.

11 Articles 85-91.

12 Article 6(1)(c).

13 Article 10.

14 Article 17.

15 Articles 49(4) and (5).

The consistency mechanism in the Regulation and the actions of the Board should hopefully narrow these gaps over time.

### New concepts - Guidance will be important

Although the Regulation has now been published, there is still uncertainty about what it means. Some provisions feel like they are the product of political compromise, rather than clear regulatory intent.

For example, an organisation must appoint a data protection officer if its core activities consist of “large scale” monitoring of individuals. Similarly, they must carry out a privacy impact assessment where new processing involves the “systematic and extensive evaluation” of individuals resulting in legal effects or significantly affects those individuals.<sup>16</sup> See *New concepts*. Getting to grips with these concepts may take time.

Clear guidance from supervisory authorities of the Board will be crucial. The Article 29 Working Party has issued a work plan<sup>17</sup> setting out four priority areas for guidance:

- > the new right to “data portability”;
- > the notion of “high risk” and privacy impact assessments;
- > certification; and
- > the role of the data protection officer.

The Article 29 Working Party will also hold workshops with stakeholders in July 2016 to further explore how best to prepare for the Regulation.

### Use of recitals

A final concern 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<sup>18</sup> (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.<sup>19</sup> They can be used to help interpret a rule (so long as it not contrary to its wording), but cannot themselves constitute a rule.<sup>20</sup>

Some of the recitals in the Regulation test the boundaries of these principles. For example, where an entity is based outside the Union they must, in most cases, appoint a representative in the Union. The recitals state that enforcement action can be taken directly against a representative<sup>21</sup>, but there is no corresponding provision in the articles of the Regulation. 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.

### FAQ

#### Does the “one stop shop” mean I am just subject to supervision by my home regulator?

The EU Commission’s plans for a “one stop shop” approach to regulation have been watered down. If you carry out cross border processing, you will be primarily regulated by the supervisory authority based in the jurisdiction of your main establishment. However, the “one stop shop” does not apply where processing is based on the legal obligation or public function condition and other supervisory authorities can ask to take control where the processing mainly relates to their jurisdiction. The lead supervisory authority can refuse to cede control, but must co-ordinate its activities closely with other ‘concerned supervisory authorities.

### 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 Regulation. Consider lobbying Member States to introduce new laws (if necessary).
- Work out where your main establishment is and who your lead supervisory authority will be.

<sup>16</sup> Articles 35 and 37.

<sup>17</sup> Statement on the 2016 action plan for the implementation of the General Data Protection Regulation, WP236.

<sup>18</sup> Recitals 32, 42 and 43.

<sup>19</sup> *Deutsches Milch-Kontor* (C-136/04).

<sup>20</sup> *Casa Fleischhandels v BALM* (C-215/88).

<sup>21</sup> Recital 80.



# Extra-territorial reach

## ! Key points

- > The Regulation primarily applies to businesses established in the Union.
- > However, it will also apply to businesses based outside the Union that offer goods and services to, or monitor, individuals in the Union.
- > These businesses will need to appoint a representative in the Union, subject to certain limited exemptions. The representative may have to accept liability for breaches of the Regulation.

## ? FAQ

### Can I appoint a European group company as my representative?

Yes. In many cases, this will be the most attractive option. The group company may be more prepared to accept the liability that comes with the role of representative.

### Caught by the Regulation - Establishment

The Regulation primarily applies to businesses established in the Union. Establishment means an effective and real exercise of activity through stable arrangements in the Union.<sup>22</sup> The legal form of the establishment is not a determining factor and could be through a branch or a subsidiary.

This is broadly similar to the test under the current Data Protection Directive, as set out by the Court of Justice in *Weltimmo* (C-230/14). However, *Weltimmo* also states that “even a minimal” establishment is sufficient. This has not been carried over to the Regulation. It is therefore not clear if a de minimis threshold will apply to the size of establishment.

The Court of Justice adopted a broad interpretation of establishment in its judgment in *Google Spain* (C-131/12). It decided that US incorporated Google Inc. was established in the Union because its activities were inextricably linked to the activities of its Spanish subsidiary Google SL.

It is not clear if this interpretation will also apply under the Regulation, i.e. that an entity outside the Union might be subject to the Regulation because of the activities of a separate legal entity in the Union. Arguably, the *Google Spain* decision was a response to a gap in the law and has been superseded by the express extra-territorial reach of the Regulation.

### Caught by the Regulation - Extra-territorial effect

One of the most significant changes in the Regulation is to extend the reach of European data protection laws to business based outside the Union. Controllers and processors will be caught where the processing activities relate to<sup>23</sup>:

- > the offering of goods or services to individuals in the Union. This appears to be closely based on the “directed at” test in the Rome I and Brussels Regulation (see *When do you offer goods or services to individuals in the Union?*).<sup>24</sup> It captures both free and paid for goods and services; and
- > monitoring the behaviour of individuals in the Union. It is less clear what this provision means. The recitals refer to individuals being tracked on the internet for profiling purposes.<sup>25</sup> Arguably it could apply broadly to any business that profiles its customers to offer personalised recommendations. However, it seems more likely this means more intrusive activities such as tracking individuals across multiple sites or using Apps to track an individual's location.

In either case, the Regulation will only apply to personal data about individuals in the Union. As under the Data Protection Directive, the nationality or habitual residence of those individuals is irrelevant.

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

#### 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 Union (if the same as the language of your home state) should not by itself make you subject to the Regulation. 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 Regulation:

- > *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* - You use references to individuals in a Member State 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 newspaper).

#### In contrast the following are weaker indications that you are offering goods or services to individuals in the Union:

- > you accept payment using a credit card with a billing address in the Union;
- > you deliver goods or services electronically to an individual who might be in the Union;
- > your internet or email advertising is not targeted at individuals in the Union, but might be seen by them; or
- > the telephone numbers on your website have an international prefix.

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?<sup>26</sup>

### Extra-territorial application to processors

One interesting question is how these extra-territorial provisions apply to processors. There are some instances in which overseas processors will be obviously caught. For example, a US company offering a consumer cloud service in Europe would clearly be caught.

However, in most cases the overseas processor is only acting on the instructions of a controller, so would not be dealing with individuals in the Union of its own volition. This does not shield it from the Regulation and it might still be caught where:

- > it is dealing with a controller or processor based in the Union. This is because the processor is processing personal data “*in the context of the activities of*” a controller or processor in the Union.<sup>27</sup> In other words, any provision of services to an entity in the Union might bring the overseas processor within the scope of the Regulation; or
- > it supplies services to a controller or processor who in turn supplies services to provide goods or services to, or monitor, individuals in the Union. In particular, the processor’s activities arguably “*relate to*” that offering of goods or services, or monitoring.<sup>28</sup> Therefore, in some cases, an overseas processor might be caught even if it only deals with entities based outside the Union.

Whether the Regulation would be applied to processors further down the supply chain in practice remains to be seen but it demonstrates the reach of the Regulation is potentially extensive.

<sup>22</sup> Recital 22.

<sup>23</sup> Article 3.

<sup>24</sup> Recital 23 and *Hotel Alpenhof GesmbH v Oliver Heller* (C-269/95).

<sup>25</sup> Recital 24.

<sup>26</sup> Recital 23.

<sup>27</sup> Article 3(1).

<sup>28</sup> Article 3(2).

## Appointment of a representative

Where these extra-territorial provisions apply, the controller or processor must appoint a representative.<sup>29</sup> 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.

This is an onerous role to take on. The representative will have to face off to the relevant supervisory authorities and accept liability for breach of the Regulation,<sup>30</sup> which could now be substantial (see *Sanctions*).

Its 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 Union, but, even then, the group company will need to consider if it is really in its interests to take on this role.

Similarly, third party service providers may be prepared to take on the role. However, they may 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?

We are not aware of any third parties currently offering to act as representative. Given the representative may have to accept liability for breach of the Regulation, it is not a role to be taken on lightly.

### ✓ To do

- ✓ Evaluate if your business (if established outside the Union) is caught by the Regulation.
- ✓ Consider if you want to take steps to avoid being subject to the Regulation, e.g. taking active steps to avoid dealing with individuals in the Union.
- ✓ If you are established outside the Union but caught by the Regulation, identify and appoint a representative in the Union (unless exempt).

<sup>29</sup> Article 27.

<sup>30</sup> Recital 80.

# Core rules remain the same

## ! Key points

- > The Regulation retains the same core rules as the 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 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. For example, it will be much harder to get a valid consent.
- > The concept of sensitive personal data has been retained and expanded to include genetic and biometric data. It will also become much harder to process information about criminal records in some Member States.

## ? FAQ

### So nothing has really changed?

The core rules are broadly the same. The Regulation will look quite familiar to experienced privacy practitioners. But this is a trap for the unwary; there are some significant changes. In addition, the Regulation 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.

### It is over twenty years since the Data Protection Directive came into force. During that time, the technical environment has changed beyond recognition

The emergence of the internet, search engines, social media, smartphones and cloud computing has led to three fundamental challenges to data protection laws:

- > First, most data is no longer stored in a structured database. Instead, it consists of unstructured electronic information such as emails, messages or photos. Applying traditional data protection laws to unstructured data is challenging.
- > Secondly, there has been an explosive growth in the volume of data. More data has been created in the past two years than in the entire previous history of the human race.<sup>31</sup>
- > Thirdly, data no longer respects national boundaries. The internet allows information to flow around the world seamlessly and instantaneously.

The Regulation was intended to address these challenges whilst ensuring a strong and coherent framework. However, it does not fundamentally change any of the core rules in the Data Protection Directive and instead develops the law incrementally by introducing a range of new obligations to support those core rules.

These additional obligations will be familiar in some Member States. For example, Germany already imposes an obligation to appoint data protection officers, has the concept of pseudonymised data and has extensive requirements for processors contracts. In other Member States, these obligations will be very new.

### Core definitions

The Regulation applies to the processing of personal data by a controller or a processor.<sup>32</sup>

These concepts are broadly the same as those under the Data Protection Directive (see *Existing concepts*). In particular, the Regulation retains the very broad definition of personal data and processing.

The Regulation 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.<sup>33</sup>

It also retains the idea that all processing is carried out by a person acting as controller (i.e. someone who determines the purpose and means of processing) or processor (i.e. someone who acts on the controller's instructions). This distinction has been criticised as it can be difficult to work out whether someone acts as controller or processor, particularly in complex relationships. However, the Regulation retains the dichotomy.

### Processing conditions

A controller must comply with all six general principles when processing personal data (see *Processing principles and conditions*). The controller must also satisfy at least one processing condition. Where sensitive personal data is processed, at least one sensitive personal data processing condition must also be satisfied.<sup>34</sup>

These core rules are very similar to those in the Data Protection Directive. However, there are some significant changes such as the restrictions on obtaining consent (see *Consent and children*) and the other changes discussed below.

<sup>31</sup> <http://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#3025f3a6c1d3>

<sup>32</sup> Article 2(1).

<sup>33</sup> Article 2(1).

<sup>34</sup> Articles 5, 6 and 9.

### Why processing conditions really matter

Under the Regulation it will be much more important to clearly understand and identify the processing condition you are relying on. In particular:

- > *Privacy Notices* - You must identify the processing condition you are relying on in your privacy notice. If you are relying on the legitimate interests condition, you must include details of that legitimate interest. If you are relying on consent, you must inform individuals of the right to withdraw consent.<sup>35</sup>
- > *Individual Rights* - The processing condition you rely on has an important effect on the rights available to individuals, for example, whether the individual has a right to object to your processing or has a right to data portability.<sup>36</sup>
- > *Jurisdiction* - The one stop shop mechanism does not apply where processing is carried out on the basis of the legal obligation or public functions condition.<sup>37</sup>

### FAQ

#### Can I carry out criminal record checks on employees?

Information about criminal convictions can only be used pursuant to Union or Member State law (or under the control of an official authority). Therefore, you would need to confirm that there is a relevant law in your Member State to justify that processing.

### Information about criminal offences

Information about criminal convictions can **only** be used pursuant to Union or Member State law, or under the control of an official authority.<sup>38</sup> There are no other justifications. Even consent from the individual will not provide a justification under the Regulation to process this type of personal data.

This is a significant change for some Member States which currently treat information about criminal offences in the same way as other sensitive personal data and thus allow processing where a sensitive personal data processing condition is satisfied.

The most obvious effect of this change is criminal record checks, which are carried out by employers in some Member States to vet new employees. These checks will only be possible under the Regulation if expressly authorised by law. For example, in the UK, the Police Act 1997 is likely to provide a sufficient basis for standard and enhanced criminal record disclosures but may not be sufficient for basic disclosure.

### Pseudonymised data and other “risk based” concepts

While much of the Regulation 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 to try and ensure the obligations in the Regulation apply in a proportionate manner, relative to the risk of the processing.

The Regulation also introduces the concept of “pseudonymised data”. This concept already exists under German data protection law and was originally proposed as a radical third class of personal data that would be regulated in a completely different way. Under the Regulation, it ends up as an important and useful privacy-enhancing mechanism, but does not materially change the core rules in the Regulation.

<sup>35</sup> Articles 13(1)(c) and (d), 13(2)(c), 14(1)(c) and 14(2)(c) and (d)].

<sup>36</sup> Articles 20 and 21.

<sup>37</sup> Articles 6(1)(c), (e) and Article 55(2).

<sup>38</sup> Article 10.



### Who is a public authority?

The Regulation applies a number of special rules to public authorities. For example, a public authority must appoint a data protection officer (see *Data Protection Officer*) and cannot rely on the legitimate interests test (see overleaf). 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”*<sup>39</sup>

It potentially includes not only the traditional emanations of the state, but also some private sector entities such as utility companies.

### 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*”.<sup>40</sup> 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).<sup>41</sup>

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?

The Regulation 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*).<sup>42</sup> They are also subject to greater restrictions when transferring personal data outside the Union.<sup>43</sup>

Finally, the definition of public authority is potentially quite broad (see *Who is a public authority?*). It could include commercial subsidiaries of public authorities as well as entities carrying out public functions such as utility companies.

### Out of scope

Some types of processing fall outside the Regulation altogether. The Regulation does not apply to processing:<sup>44</sup>

- > 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.<sup>45</sup> However, controllers or processors providing those social networks are subject to the Regulation;
- > 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 Union law (e.g. national security);
- > for the purpose of the Union’s foreign and security policy; and
- > by Union institutions. Those institutions are subject to Regulation 45/2001 on the processing of personal data by Community institutions.

### ✓ To do

- Review your existing compliance.
- Work out if you are processing genetic or biometric information, or information about criminal offences. If so, bring that processing into line with the new requirements of the Regulation.

<sup>39</sup> *Foster and others v British Gas* (C-188/89).

<sup>40</sup> Article 6(1).

<sup>41</sup> Article 6(1)(e).







<sup>42</sup> Article 37(1)(a).

<sup>43</sup> Article 49(3).

<sup>44</sup> Article 5(2).

<sup>45</sup> See recital 18. This appears to expand the scope of this exemption. Currently those using social networks are potentially subject to the Data Protection Directive under the principles in the *Lindqvist* (C-101/01) case.

## Existing concepts

<p><b>Personal data</b> </p> <p>Personal data is:</p> <ol style="list-style-type: none"> <li>1. information;</li> <li>2. relating to;</li> <li>3. an identified or identifiable;</li> <li>4. natural person.</li> </ol> <p>It is a broad term and includes a wide range of information.</p> <p>The Regulation expressly states this includes online identifiers such as IP addresses and cookie identifiers. However, this is already likely to be the case under the Data Protection Directive (see the Advocate General's opinion in <i>Breyer C-582/14</i>).</p>	<p><b>Sensitive personal data</b> </p> <p>This is personal data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.</p> <p>The inclusion of genetic and biometric data is new.</p> <p>Information about criminal convictions and offences is treated separately and subject to even tighter controls.</p>
<p><b>Controller</b> </p> <p>This is a person who, alone or jointly with others, determines the purposes and means of the processing of personal data.</p> <p>In other words, the controller decides "what" personal data will be processed for and "how" it will be done.</p>	<p><b>Processor</b> </p> <p>This is a person who processes personal data on behalf of a controller.</p> <p>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 in practice to work out if someone acts as controller or processor. Unlike under the Data Protection Directive, processors will become directly liable for compliance with some parts of the Regulation.</p>
<p><b>Data subject</b> </p> <p>The data subject is the natural person to whom the personal data relates.</p> <p>We refer to them as "individuals" in this report.</p>	<p><b>Processing</b> </p> <p>Processing is a very broad concept and includes almost anything you can do with personal data, including collection, use, storage and destruction.</p> <p>Disclosure is one form of processing, but the definition is much wider than that.</p>

## New concepts

### Pseudonymised data



**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.

**Relevance:** Pseudonymised personal data is not exempt from the Regulation. However, it may be easier to justify the processing of pseudonymised personal data. For example, the Regulation 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.

### Large scale processing



**Meaning:** There is relatively little guidance on what large scale processing means. The Regulation suggests that it means processing a considerable amount of personal data at regional, national or supranational level and 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.

**Relevance:** This concept is also a factor in determining whether obligations under the Regulation 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 Union, but caught by the Regulation, 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 processing sensitive personal data or monitoring public areas on a “large scale”.

### Risk to individuals



**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 the reputation or reversal of pseudonymisation. 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.

**Relevance:** This is an important concept and arises at several points in the Regulation. 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 Union, but caught by the Regulation, need to appoint a representative in the Union.

### High risk to individuals



**Meaning:** There is relatively little guidance on when processing will be of high risk to individuals. In relation to privacy impact assessment, processing may be high risk if it prevents data subjects from exercising a right or using a service or a contract, or because it is carried out systematically on a large scale. The Article 29 Working Party has said it will issue guidance on this concept shortly.

**Relevance:** This concept is the trigger for a number of further obligations under the Regulation. For example: (a) individuals must be told of data breaches if they are likely to be “high risk”; and (b) privacy impact assessments are needed if the processing is likely to result in a “high risk” for individuals.

## Processing principles and conditions

### The six general 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 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.

### In practice

**The six general principles:** These obligations are all but identical to the obligations under the Data Protection Directive. On the whole, they represent good business practice. One important change is a new obligation on controllers to not only comply with these principles but be able to show they comply. This is an important part of the new accountability obligations (see *Accountability*).

**Sensitive personal data processing conditions:** Identifying a processing condition for sensitive personal data will continue to be challenging in some situations (as it was under the Data Protection Directive). In some cases, controllers will need to take a pragmatic and robust approach to interpreting these conditions, focusing particularly on processing of sensitive personal data that might potentially harm individuals.

**Processing conditions:** These gateways are broadly similar to those under the Data Protection Directive. However:

- > it will become much harder to obtain consent (see *Consent and children*), meaning that controllers will have to fall back on other conditions; and
- > public authorities cannot use the legitimate interests condition.

In a number of cases, controllers will have to rely on the legitimate interests test condition. This involves a “careful assessment of”<sup>46</sup> the underlying processing to ensure it properly balances the interest of the controller against any potential intrusion to the individual’s privacy. In particular, would the individual “reasonably expect” processing for that purpose will take place. There are a number of provisions in the recitals identifying activities that are legitimate (e.g. processing for direct marketing, preventing fraud, cyber security and intra-group transfers<sup>47</sup>) but step change in sanctions makes this a much “bigger call”. There is a risk of a chilling effect if controllers are not confident to proceed with processing activities on the back of what is, essentially, a subjective value judgement.

### 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 Regulation;
- 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 Union or Member State law will satisfy this condition. However, that law need not be statutory (e.g. common law obligations are sufficient);
- d. *Vital interests* - The processing is necessary in order to protect the vital interests of the individual or of 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 rely on this condition.

### Processing condition - Sensitive personal data (Article 9(2))

The Regulation places much stronger controls on the processing of sensitive 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, Union 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 of 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 Union 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 Union or Member State law; or
- j. *Archive* - The processing is necessary for archiving, scientific or historical research purposes or statistical purposes and is based on Union or Member State law.

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

46 Recital 47.

47 Recitals 47-49.

# Consent and children

## ! 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 Regulation. Individuals can also withdraw their consent at any time.
- > As under the Data Protection Directive, consent to process sensitive personal data must be explicit. Consent to transfer personal data outside the Union 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 - e.g. you can easily not process that personal data if the individual does not provide consent or subsequently withdraws their consent.

### Under the Regulation, it will become much more difficult to obtain a valid consent

The Regulation 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 principles and 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 Regulation. For example, ensuring that you are not using pre-ticked boxes and

### 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:**<sup>48</sup>

- > *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.
- > *Consent to all purposes* - If the relevant processing has multiple purposes, consent must be given for all of them. The meaning of this provision is not clear. At one extreme it might prevent mixed justifications for different activities. For example, it would not be possible to rely on performance of a contract when providing services to an individual and obtain a separate ancillary consent for direct marketing. You would need a (valid) consent for them all.
- > *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.
- > *Unbundled consent* - 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 sensitive personal data or transferring personal data outside the Union. 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.

that ensuring the request for consent is separate from other matters.

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 has been given under the Data Protection Directive, it will continue to be valid under the Regulation if it also meets the requirements of the Regulation.<sup>49</sup> This may be difficult given the new and stringent requirements for consent.

In theory, some businesses should therefore consider approaching their existing customers or employees to obtain a fresh consent that is valid under the Regulation. However, this is likely to be an onerous exercise and in many cases will not lead to a fresh consent.

### Consent and marketing

The ePrivacy Directive imposes additional constraints if you market by telephone, email or fax.<sup>50</sup> 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 currently defines consent by reference to the Data Protection Directive. This will automatically be superseded by a reference to the Regulation from May 2018 onwards.<sup>51</sup> In other words, obtaining consent to market by email will become a whole lot harder as well.<sup>52</sup>

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.

### 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 really matter*), this could lead to some curious privacy notices. For example having to tell your customers they “consent” to certain disclosure under banking secrecy laws but only “acknowledge” their personal data will be processed under the Regulation, for which a different processing condition will apply.

## 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, i.e. have their data erased (see *Data subjects' rights*). However, withdrawal of consent does not affect the lawfulness of any processing that takes place prior to that withdrawal.

48 Article 7 and recitals 32, 42 and 43.

49 Recital 171.

50 ePrivacy Directive, Article 13.

51 Article 94(2).

52 Though interestingly, Article 95 states that the Regulation 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 Regulation 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.<sup>53</sup>

The Regulation 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.<sup>54</sup> The Regulation expressly states that consent is not necessary when providing preventive or counselling services to a child.<sup>55</sup>

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

- > your privacy policies must be very clear and simple if they are aimed at children;<sup>56</sup>
- > importantly, profiling and automated decision making should not be applied to children;<sup>57</sup> and
- > the right to be forgotten applies very strongly to children.<sup>58</sup>

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

### To do

- Review your existing processes to obtain consent to determine if they are valid under the Regulation.
- Consider 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.

53 Article 8.

54 Article 6(1)(f).

55 Recital 38.

56 Recital 58.

57 Recital 71.

58 Recital 65.





# Data subjects' rights

## ! Key points

- > The Regulation largely preserves the existing rights of individuals to access their own personal data, rectify inaccurate data and challenge automated decisions about them. The Regulation 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. The new rights are complex and it is not clear how they will operate in practice.

## ? 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.

## One of the key aims of the Regulation 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. In the short term, these rights are likely to cause confusion amongst controllers and could be a disappointment for individuals.

## New rights - Right "to be forgotten", restrict processing and to object

These three rights<sup>59</sup> are both complicated and closely interlinked.<sup>60</sup> The flowchart overleaf sets out how these rights work. If you operate a consumer-facing business, it is very likely you will start to receive these requests. You should start to 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 to stop processing the personal data and to erase, or at least quarantine, that personal data. These combination requests will inevitably be more difficult to handle.

## New rights - Data portability

Individuals already 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.<sup>61</sup> Individuals can also ask for the data to be transferred directly from one controller to another. There is no right to charge fees for this service.

However, the right:

- > only applies to personal data "provided to" the controller. This will clearly apply to photos posted to a social network or content stored on a cloud service. Whether it includes other types of information, for example details of purchases or transaction histories, is less clear. Arguably this content is created by the controller, not provided to them; and
- > only applies where the controller is processing personal data in reliance on the processing conditions of consent or performance of a contract.

In practice, this will be a useful right for individuals in limited situations, such as transferring between social networks or cloud providers. Its application in other situations is not clear.

## Existing rights - Right to object to direct marketing

The Regulation preserves the right for individuals to object to direct marketing.<sup>62</sup>

As under the Directive, when an individual exercises this right, you must not only stop sending direct marketing material to the individual, but also stop any processing of that individual's personal data for such marketing. For example, if you receive an objection, you should stop profiling that individual to the extent related to direct marketing. The reference to profiling here is new and it is not clear if this is intended to create a wide ranging opt-out from profiling (which would be wider than the express provisions on profiling, see below) or just an opt-out to profiling that leads to direct marketing to the individual concerned.

The ePrivacy Directive contains additional restrictions on marketing and in some cases requires the consent of the individual. The ePrivacy Directive will continue to apply in parallel with the Regulation, but will become more difficult to comply with given the additional restrictions on obtaining consent (see *Consent and children*).

## Existing rights - Subject access requests

Individuals will still be able to make a subject access request to obtain copies of their personal data. The Regulation makes the following amendments:

- > *Free* - You must respond to the subject access request for free. This may increase the volume of requests. However, you can charge if the individual asks for further copies of the personal data.<sup>63</sup>
- > *Excessive requests* - You can refuse to respond to the request if it is manifestly unfounded or excessive (or charge an administrative fee). The Regulation states that where large volumes of personal data are processed, the individual should specify exactly what information or processing their request relates to. However, it is not clear how far this protects the controller from unreasonable subject access requests, for example if it will still be necessary to trawl emails to respond to subject access requests (something currently necessary in some Member States). In addition, you will have the burden of proving the request is manifestly unfounded or excessive.<sup>64</sup>
- > *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.<sup>65</sup>
- > *Purpose of requests?* The request should allow the individual to be aware of and verify the lawfulness of the processing you are carrying out.<sup>66</sup> It is not clear if this would allow you to push back on requests that are not made for this purpose, as is potentially the case under the Directive.<sup>67</sup>
- > *Time to respond* - You have a month to respond to the subject access request. You can extend this by a further two

months if the request is complex or if you have received a large number of requests.

- > *Right to withhold* - You can withhold personal data if disclosure would “adversely affect the rights and freedoms of others”.<sup>68</sup> This repeats similar provisions in the Data Protection Directive but the rights and freedoms recognised in the Union have changed since that Directive was passed. In particular the Charter of Fundamental Rights 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.<sup>69</sup> Member States are likely to introduce further national derogations for personal data that benefits from legal privilege or that would prejudice law enforcement, regulatory or judicial functions.

Subject access requests are heavily used in some jurisdictions. Working out the answers to these questions is likely to cause significant friction as the Regulation beds in.

## 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.<sup>70</sup> 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 Union or Member State law.

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

These rules are very similar to those in the Data Protection Directive. While earlier drafts of the Regulation promised a much broader clamp down on profiling, the final position is much more moderate. For example, in many cases, profiling for marketing purposes will fall outside this restriction as it is unlikely to have legal effects or significantly affect the individual.<sup>71</sup> Individuals may however have a right to object to profiling for direct marketing (see above).

## Time for compliance

You must comply with the exercise of these rights within a month. If the request is complex or you have received a large number of requests, you can extend this period by a further two months.<sup>72</sup>

### To do

- Consider if individuals are likely to exercise these rights against you and what they mean for your business in practice.
- Based on that analysis, set up processes to capture, record and act on those requests.

<sup>59</sup> The right to object already exists under the Directive but will be much stronger under the Regulation.

<sup>60</sup> Articles 17, 18 and 21.

<sup>61</sup> Article 20.

<sup>62</sup> Article 21(3).

<sup>63</sup> Article 12(5).

<sup>64</sup> Article 12(5) and recital 63.

<sup>65</sup> Article 15(3) and recital 63.

<sup>66</sup> Recital 63.

<sup>67</sup> See *YS v Minister voor Immigratie* (C-141/12 & C-372/12).

<sup>68</sup> Article 15(4).

<sup>69</sup> Recitals 4 and 63.

<sup>70</sup> Article 22.

<sup>71</sup> Recital 71 suggests that refusal of online credit or automated vetting of employment applications are the sorts of processing caught by these provisions.

<sup>72</sup> Article 12(3).

## Data subjects' rights

	When does the right apply?	Exemptions
The right to object	<p>You must comply with the request where your processing is based on one of the following processing conditions:</p> <ul style="list-style-type: none"> <li>&gt; public interest; or</li> <li>&gt; the legitimate interest condition.</li> </ul>	<p>You do not need to comply if the processing is:</p> <ul style="list-style-type: none"> <li>&gt; for legal claims; or</li> <li>&gt; based on a compelling legitimate interest which override the interests of the individual</li> </ul>
The right to erasure / "right to be forgotten"	<p>You must comply with the request where:</p> <ul style="list-style-type: none"> <li>&gt; the individual has <b>objected</b> to the processing and (other than in relation to objections to direct marketing) there are no overriding legitimate grounds to justify that processing;</li> <li>&gt; the personal data is no longer needed for the purpose for which it was collected or processed;</li> <li>&gt; the individual withdraws consent and there are no other grounds for the processing;</li> <li>&gt; the personal data is unlawfully processed;</li> <li>&gt; there is a legal obligation under Union or Member State law to erase the personal data; or</li> <li>&gt; personal data was processed in connection with an online service offered to a child.</li> </ul>	<p>You do not need to comply if the processing is:</p> <ul style="list-style-type: none"> <li>&gt; necessary for rights of freedom of expression or information;</li> <li>&gt; for compliance with a legal obligation under Union or Member State law;</li> <li>&gt; in the public interest or carried out by an official authority;</li> <li>&gt; for public interest in the area of public health;</li> <li>&gt; for archiving or research; or</li> <li>&gt; for legal claims.</li> </ul>
The right to restrict processing	<p>You must comply with the request where:</p> <ul style="list-style-type: none"> <li>&gt; the individual has <b>objected</b> to the processing and you are considering if there are overriding legitimate grounds that justify continued processing;</li> <li>&gt; the processing is no longer necessary but retention is needed to deal with legal claims;</li> <li>&gt; the processing is unlawful but the individual wants the data to be restricted not erased; or</li> <li>&gt; the accuracy of the personal data is being contested and the controller is verifying that data.</li> </ul>	None.

**What must you do?**

You must **stop processing** that individual's personal data.

**Commentary**

*The right to object is similar to the existing right in the Data Protection Directive.*

*However, the Regulation 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).*

You must **erase** 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.

*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.*

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

## ! Key points

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

## 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. A recent study found it would take the average internet user 76 days to read all of the privacy notices they encounter in a year.<sup>73</sup> Many privacy policies are too long and too complex. The same study found that the median length of the policies reviewed was approximately 2,500 words.

## Approach in the Regulation

The Regulation does nothing to resolve this tension and instead makes the position worse. It requires controllers to:

- > ensure their privacy notices are “concise, transparent, intelligible and easily accessible”;<sup>74</sup> 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?

## 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:<sup>75</sup>

- > 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:<sup>76</sup>

- > 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 Union 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 Regulation 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 Regulation 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.<sup>77</sup>

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

### To do

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

<sup>73</sup> The Cost of Reading Privacy Policies, Aleecia M. McDonald and Lorrie Faith Cranor, 2012.




<sup>74</sup> Article 12(1).

<sup>75</sup> Article 13(1) and 14(3).

<sup>76</sup> Article 14(5).

<sup>77</sup> Articles 12(7) and (8).

## Information you must include in your privacy notice

Requirement	Commentary
<input checked="" type="checkbox"/> Your identity, contact details and details of your representative (if any).	 The provision of this information is straightforward.
<input checked="" type="checkbox"/> The contact details of your data protection officer.	 The provision of this information is straightforward.
<input checked="" type="checkbox"/> The purpose and legal basis of processing. Where legitimate interests is relied upon, details of those interests.	 The need to describe the legal basis for any processing is new. It reflects the importance the Regulation places on accurately identifying the processing condition you rely on (see <i>Why processing conditions really matter</i> ).
<input checked="" type="checkbox"/> The right to withdraw consent (if this is the basis for any processing).*	 The provision of this information is straightforward. Dealing with requests to withdraw consent may not be (see <i>Consent and children</i> ).
<input checked="" type="checkbox"/> The categories of personal data processed.† <input checked="" type="checkbox"/> The recipients or categories of recipients of personal data.	 It is not clear how detailed this information has to be. Although this information is commonly used in existing privacy notices, its inclusion is not mandatory.
<input checked="" type="checkbox"/> The source of the personal data, including use of public sources.‡	 A comprehensive description of all categories of personal data processed, together with all sources <sup>78</sup> and recipients could be long and difficult to prepare. See <i>Accountability</i> for a discussion of this issue in relation to record keeping.
<input checked="" type="checkbox"/> Details of any intended transfer outside the Union. Details of any safeguards relied upon and the means to obtain copies of transfer agreements.	 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 Union.
<input checked="" type="checkbox"/> The period for which data will be stored or the criteria used to determine this period.*	 Much depends on how detailed this information needs to be. Most businesses hold a wide variety of personal data, so it will be difficult to provide a comprehensive description of exactly how long each type of personal data will be stored for.
<input checked="" type="checkbox"/> A list of the individual's rights, including the right to object to direct marketing, make a subject access request, and to be "forgotten".*	 The provision of this information is straightforward. Dealing with individuals exercising these rights may not be (see <i>Data subjects' rights</i> ).
<input checked="" type="checkbox"/> Details of any automated decision making, including details of the logic used and potential consequences for the individual.	 The obligation to disclose "meaningful information about the logic used" in any automated decision making may be challenging.
<input checked="" type="checkbox"/> Whether provision of personal data is a statutory or contractual requirement, whether disclosure is mandatory and the consequence of not disclosing personal data.*‡	 The provision of this information is straightforward.
<input checked="" type="checkbox"/> The right to complain to a supervisory authority.*	 The provision of this information is straightforward.

\* 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, we would normally expect it to 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.

78 Recital 61 states that it may be sufficient to provide 'general information' on sources.



# Accountability

## ! Key points

- > Under the Regulation, you must not only comply with the six general 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 Regulation, by signing up to a Code of Practice or becoming Certified.

## ? FAQ

### How can I “demonstrate” I am complying with the Regulation?

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.

### The Regulation will require you not just to comply, but to be seen to comply

New concepts, such as accountability,<sup>79</sup> 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 policies 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 Regulation 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<sup>80</sup> (albeit not actually file those records with the supervisory authority).

Details of these record keeping obligations are set out in the table opposite. The key issue is how detailed this information needs to be. The current notification obligations vary from Member State to Member State with some only asking for very brief and high level information (such as the UK) and others asking for more detailed information on a database-by-database basis (such as France).

If the Regulation requires a detailed description of all the processing carried out by a controller, this will be a significant additional burden in some Member States and will require a bottom up audit of all processing conducted by that business, together with a process to maintain and update that information.

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.<sup>81</sup> This exemption will therefore be rarely used.

## 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 applicable);
- > a general description of the security measures employed (where possible).

<sup>79</sup> Article 5(2).

<sup>80</sup> Article 30.

<sup>81</sup> Article 30(5).

## Privacy impact assessment

Many businesses already incorporate privacy impact assessments into their product development cycle. The Regulation 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”.<sup>82</sup> The Regulation sets out some examples of when processing is high risk. Those examples suggest assessments will only be needed in relatively limited circumstances. The Article 29 Working Party is producing further guidance on this point, which might raise or lower this threshold.
- > *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*”.<sup>83</sup> The wording here is curious. It appears to suggest that mitigating steps should be ignored when assessing whether to consult the supervisory authority. However, based on the recitals, we think a more purposive interpretation should be used and consultation is only required if the risk cannot be mitigated.<sup>84</sup>
- > *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 Regulation envisages co-regulation through the development of private sector Codes of Conduct or Certification.<sup>85</sup> 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 Regulation by clarifying exactly what the general requirements in the Regulation mean in a particular sector or in relation to a particular type of processing (e.g. provide clarity on what security measures are appropriate). They can also be used to justify international transfers of personal data (see *Transfers outside the Union*).

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 Regulation 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 review and update your existing compliance policies. In some cases, you will need to create new policies.
- You will need to create and maintain a record of the processing you are carrying out (unless exempt).
- You should adapt your product development processes to include a privacy impact assessment, where necessary.

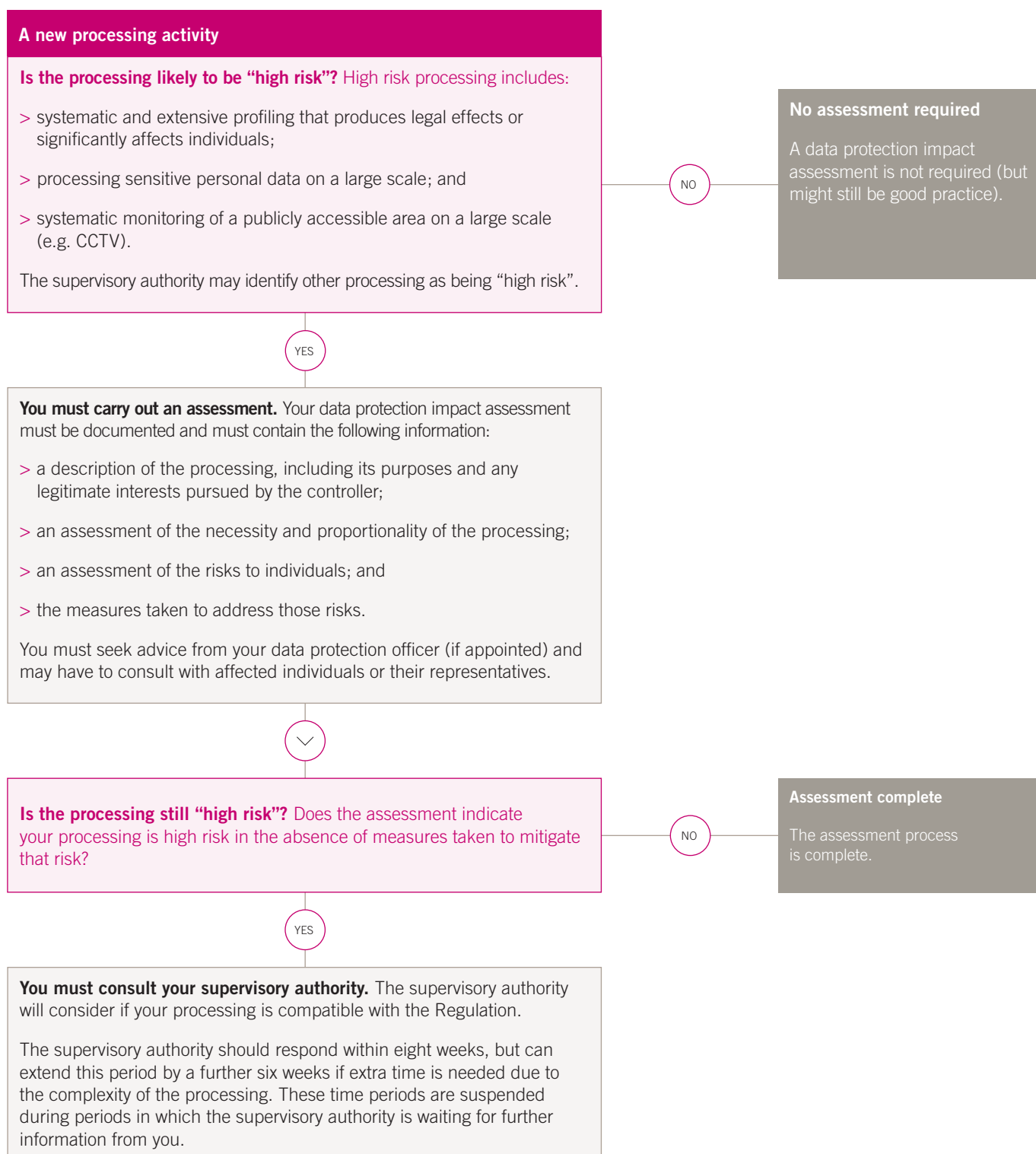
<sup>82</sup> Article 35(2).

<sup>83</sup> Article 36(1).

<sup>84</sup> Recital 94.

<sup>85</sup> Articles 40-43.

## Privacy Impact Assessments



# Data protection officer

## ! Key points

- > You may be obliged to appoint a data protection officer. This depends on the 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 business

## ? 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).

### Data protection officers are an important aspect of the accountability principle

They are a means to ensure compliance with Regulation without external intervention by the supervisory authority. They are an existing feature of many Member States' data protection laws, such as Germany.

### 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 is likely to bring all of the provisions of the Regulation 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.

### When must you appoint a data protection officer?

#### You must appoint a data protection officer if:

- > *Member State law* - You are required to do so by national law. Some Member States are likely to make this mandatory, particularly where this obligation already exists in national law (e.g. Germany);
- > *Public authority* - You are a public authority or body (other than a court);
- > *Regular and systematic monitoring* - Your core activities consist of regular and systematic monitoring of data subjects on a large scale; or
- > *Sensitive personal data* - Your core activities consist of processing sensitive personal data on a large scale (including processing information about criminal offences).

## The role of data protection officer

The data protection officer is responsible for monitoring compliance with the Regulation, providing information and advice, and liaising with the supervisory authority.<sup>86</sup> 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 (i.e. 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. There are good arguments for the data protection officer to be separate from the compliance unit and instead operate as a form of third line of defence. This avoids the risk of the data protection officer “marking their own homework”.

## 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.<sup>87</sup>

This may make a group-wide appointment difficult. For example, if the data protection officer does not speak the local language, they may not be sufficiently “accessible” for local employees or customers. Similarly, if the data protection officer is not familiar with the way the Regulation operates in that jurisdiction (i.e. the impact of national derogations) or the interaction with local law, it might be hard to demonstrate they have the expert knowledge needed to fill that role.

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 would also have to report into the highest level of management for every operating company within the group. Having multiple reporting obligations across the whole group may mitigate against the appointment of a group wide data protection officer.

## FAQ

### 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 have been dropped from the Regulation.

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

## To do

- Work out if you need to appoint a data protection officer. Even if you don't need to appoint a data protection officer, consider if you want to make a voluntary appointment.
- 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.
- Create a job specification for the role and appoint someone to that role.

<sup>86</sup> Articles 38-39.

<sup>87</sup> Articles 37(2) and (5).

# Data security

## ! Key points

- > The Regulation 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.

## ? FAQ

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

The obligations in the Regulation 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.

### Data security is a priority for most businesses

Last year saw further 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 Regulation 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 Regulation applies the same broad security obligation as the 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: <sup>88</sup>

- > 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.

These security obligations apply to processors who have the added difficulty of not always knowing what their services are being used for. For example, cloud providers will not generally know what sorts of data their customers are storing on their systems and will often be prohibited from looking at it. From a security perspective, processors may have to plan for a “worst case scenario” in which customers are using their services to store highly sensitive and personal data.

It is also worth noting these obligations do not just relate narrowly to data security but instead address wider business continuity issues.

### Notice of breach

One of the most striking changes in the Regulation is the obligation on controllers to notify the supervisory authority and, in some cases, individuals of personal data breaches. <sup>89</sup> The process is set out overleaf.

The introduction of the breach notification obligations 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.

Whether supervisory authorities are ready for the wave of notifications remains to be seen, as does the need to notify breaches within 72 hours (where feasible). Most supervisory authorities work on much longer timescales. They are unlikely to welcome a drip feed of partial information and updates from controllers as they struggle to both get to grips with a data breach and provide prompt notification to the supervisory authority.

Making a notification may also 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.

## The Network and Information Security Directive

### When will it come into force?

The Network and Information Security Directive must be implemented in Member States by 10 May 2018.

### Who does it apply to?

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 Directive; 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 Regulation. In addition, the incident does not have to involve the loss of data (i.e. it could instead cause 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.

## Centralised breach reporting units

In practice, large businesses are likely to need a centralised unit to which data breaches can be reported, analysed, recorded and the right notifications made to the right regulators.

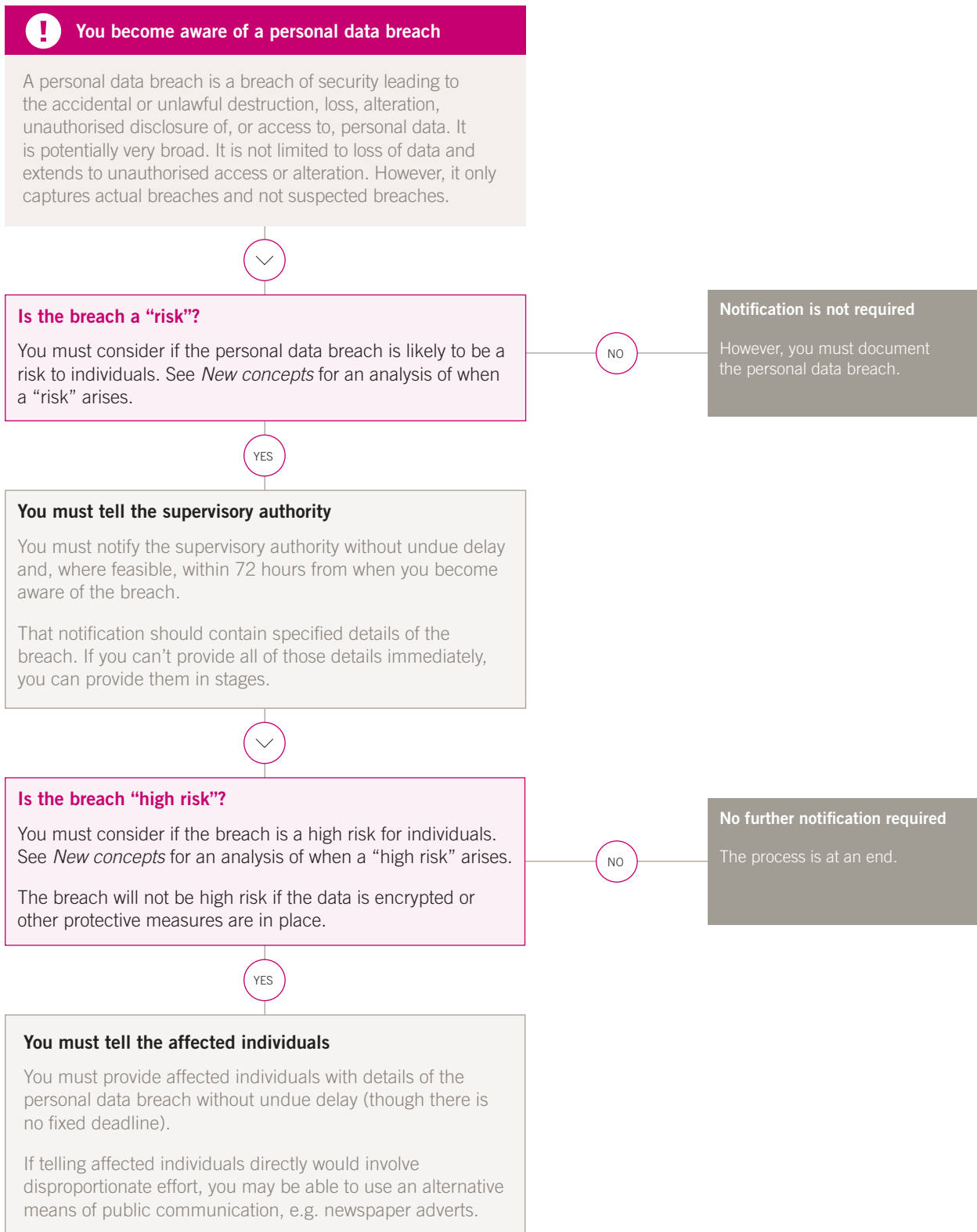
In some cases, this is potentially quite complex. You may have to make separate reports to the supervisory authority (under the Regulation), the competent authority/ CSIRT (under the Network and Information Security Directive), the telecoms authority (under the ePrivacy Directive) and other sector-specific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

Those 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 those 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.

## ✓ 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 Regulation.

## Breach notification process







# Processors

## ! Key points

- > The Regulation expands the list of provisions controllers must include in their contracts with processors.
- > Some aspects of the Regulation are directly applicable to processors. This will be a major change for some suppliers who have avoided direct regulation under the Data Protection Directive by setting themselves up as processors.
- > Processors will be jointly and severally liable with the relevant controller for compensation claims by individuals.

## ? 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*.

## New dynamic in negotiation with processors

The Regulation will apply directly to processors. This is a significant change as processors were largely exempt from regulation under the Data Protection Directive (although around 11 Member States placed at least some direct obligations on processors in their national laws). Details of the obligations placed on processors under the Regulation are set out in the table opposite.

These obligations, together with the significant increase in sanctions under the Regulation, are likely to change the negotiating dynamic between customers and service providers.

Data protection is no longer “a customer problem” and service providers will have a much greater stake in finding the right compliance solution. Service providers may also try and shift some of this liability back to customers, for example by seeking cross-indemnities in case they are sanctioned due to failings by the customer.

## Changes to your data processing contracts

The Regulation 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 impact of this change will vary from jurisdiction to jurisdiction, for example the impact for German controllers is more limited as many of these obligations are already mandatory under German law.

The Regulation also envisages that the EU Commission or supervisory authorities will issue template wording that could be used to satisfy these requirements.

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 Regulation.<sup>90</sup> This is much broader than the previous obligation under the Directive which only required controllers to confirm that their processors had adequate data security.

There is no express grandfathering of existing processing contracts so you should future-proof contracts you enter into now to meet the requirements of the Regulation. You should consider if you need to amend your existing contracts to introduce these new obligations in good time before May 2018.

## 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). However, under the Data Protection Directive it was not clear if a controller is 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, i.e. no processing condition is required. However, there is no similar provision under the Regulation and so no clear basis for disclosures of sensitive personal data to processors. In some jurisdictions at least, this will raise difficult compliance issues when using processors, such as cloud providers, for healthcare or human resources purposes.

90 Article 28(1).

## Processors and transfers outside the Union

One curious omission from the list of new processor clauses is any substantive control on transfers of personal data outside the Union. 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 Union.

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

If so, this would be a very 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.

### Obligations placed on processors

To appoint a representative if based outside of the Union.	Art. 27
To ensure certain minimum provisions in contracts with controllers (see <i>Mandatory obligations for data processor contracts</i> ).	Art. 28(3)
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.	Art. 28(2) & (4)
Only to process personal data on the instructions of the controller unless required to process for other purposes by Union or Member State law (but not foreign law, such as US law. This will be a major headache for many foreign processors).	Art. 29
To keep a record of processing carried out on behalf of a controller (see <i>Record keeping obligations</i> ).	Art. 30
To co-operate with the supervisory authorities.	Art.31
To implement appropriate security measures (see <i>Data security</i> ).	Art. 32
To notify the controller of any personal data breach without undue delay.	Art.33
To appoint a data protection officer in certain cases (see <i>Data protection officers</i> ).	Art. 37
To comply with the rules on transfers of personal data outside of the Union (see <i>Transfers outside the Union</i> ).	Art. 44

### ✓ To do

- ☑ If you act as controller, update your contract templates to include the new 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 Regulation. 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

Requirement	
<input checked="" type="checkbox"/> The contract must contain a description of: <ul style="list-style-type: none"> <li>&gt; scope, nature and purpose of processing</li> <li>&gt; duration of the processing; and</li> <li>&gt; types of personal data and categories of data subjects.</li> </ul>	<i>Art. 28(3)</i>
<input checked="" type="checkbox"/> 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 Union or Member State law, but the processor must inform the controller (unless prohibited from doing so).	<i>Art. 28(3)(a)</i> <i>Recital 81</i>
<input checked="" type="checkbox"/> The personnel used by the processor must be subject to a duty of confidence.	<i>Art. 28(3)(b)</i>
<input checked="" type="checkbox"/> The processor must keep the personal data secure.	<i>Art. 28(3)(c)</i> <i>Art. 32</i>
<input checked="" type="checkbox"/> 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.	<i>Art. 28(2)</i> <i>Art. 28(3)(d)</i>
<input checked="" type="checkbox"/> The processor must ensure it flows down these obligations to any sub-processor. The processor remains responsible for any processing by the sub-processor.	<i>Art. 28(4)</i>
<input checked="" type="checkbox"/> 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.	<i>Art. 28(3)(e)</i>
<input checked="" type="checkbox"/> The processor must assist the controller with their security and data breach obligations, including notifying the controller of any personal data breach.	<i>Art. 28(3)(f)</i> <i>Art. 33(2)</i>
<input checked="" type="checkbox"/> The processor must assist the controller should the controller need to carry out a privacy impact assessment.	<i>Art. 28(3)(f)</i>
<input checked="" type="checkbox"/> 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 Union or Member State law.	<i>Art. 28(3)(g)</i>
<input checked="" type="checkbox"/> 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.	<i>Art. 28(3)(h)</i>
<input checked="" type="checkbox"/> The processor must inform the controller if, in its opinion, the controller’s instructions would breach Union or Member State law.	<i>Art. 28(3)</i>



# Transfers outside the Union

## ! Key points

- > The Regulation prohibits the transfer of personal data outside of the Union, 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. You may continue to be stuck between a rock and a hard place.

## ? FAQ

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

The current Model Contracts are “grandfathered” under the Regulation 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 Regulation for processor contracts.<sup>91</sup> Therefore you should consider amending them as part of your general review of existing processor contracts.

### 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 Regulation 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 Union*). 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 Regulation (see *Consent and children*).
- > *Model Contracts* - In a welcome development, these will 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. Currently, they are 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 transfers 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 Union or Member State law. This does not include transfers to adequate jurisdictions, but does include transfers made on another basis, for example Model Contracts.<sup>92</sup>

### Onward transfers

Another more significant change is that the Regulation regulates not just the initial transfer to a third country but also onward transfers. Under the 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 Regulation? Presumably it would have to be the initial exporter as, in most cases, the importer will not be subject to the Regulation. 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 Regulation allows minor transfers of personal data outside the Union in certain very limited situations. It was 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 Union.

In some jurisdictions, such as the UK, it replaces the “presumption of adequacy” test. This allows 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!).

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.

#### 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

#### 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 Regulation does nothing 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 Union 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. In any event, the UK has indicated it will opt out of this provision.

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.<sup>93</sup>

Whether some supervisory authorities take a more aggressive approach to Article 48 remains to be seen. At the very least, those authorities will have much greater sanctioning powers where they feel intervention is required.

#### ✓ To do

- ✓ You should review your current transfers and consider if they are justified now and will continue to be justified under the Regulation.
- ✓ 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.

91 Recital 10 of the EU Model Contracts for processor transfers (Commission Decision C(2010)593) states that they satisfy the requirements of Article 17(3) of the Data Protection Directive in respect of processor contracts. However, it is not clear if this, in conjunction with the deeming provision in Article 94(2) of the Regulation, means they are also sufficient for the purposes of the Regulation.

92 Article 49(5)

93 Recital 115.

## Strategies for transfers of personal data outside the Union





### “Whitelisted” jurisdictions

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 Regulation. The current adequacy findings will all be grandfathered in the short term, i.e. 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. 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. Given the jurisdiction must have “essentially equivalent” laws, it is unlikely that many more findings will be made.

### Minor transfers

The Regulation 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.

### Other derogations

The Regulation also permits a transfer if it is:

- > 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 Union or Member State law;
- > 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.

### Explicit consent

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 Regulation (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

## ! 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 (e.g. 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.

## Fines

One of the aims of the Regulation 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.<sup>94</sup> These fines apply to breaches of many of the provisions of the Regulation, 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.<sup>95</sup> 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.<sup>96</sup> 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.<sup>97</sup> They will have the right to recover both material damage and non-material damage (e.g. 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.<sup>98</sup>

## What is your attitude to risk?

The Regulation applies to any processing of personal data. In the modern world, this means it touches almost everything you do. This makes it very challenging given its flexible and principle-based approach to regulation and the step change in sanctions.

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

- > *Uncertainty* - While much of the Regulation is familiar, there are a number of new provisions and it will take time to fully understand what they mean. Guidance on this issue will help, though experience indicates that not all of it will be clear or pragmatic.
- > *Value judgements* - In many cases, you will need to make a subjective judgement on whether processing is 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.
- > *Technical non-compliance* - In some cases, you will do things that clearly breach the Regulation. 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 will stop with the advent of the Regulation, so you should consider your attitude to these types of risks.

## Managing risk

The Regulation 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 - a balancing exercise that may prove difficult in practice. 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 Regulation, but you are unlikely to be a priority for enforcement.
- > *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 Regulation 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?

## FAQ

### Why can't I do [X]\*? Does the Regulation really stop me doing this?

It will not be "business as usual" when the Regulation takes effect. There will be things you are currently doing that you simply cannot do under the Regulation. However, for many activities there is no clear right or wrong answer. Instead they require a subjective assessment of the principles in the Regulation. 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.

## To do

- You should review your current level of compliance and bring it up to the level required under the Regulation.
- 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.

# To do

## Countdown to 2018

- ✓ Work out where your main establishment is and who your lead supervisory authority will be
- ✓ 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 Regulation. Consider lobbying Member States to introduce new laws (if necessary)

## Extra-territorial reach

- ✓ Evaluate if your business (if established outside the Union) is nonetheless caught by the Regulation
- ✓ Consider if you want to take steps to avoid being subject to the Regulation, e.g. taking active steps to avoid dealing with individuals in the Union
- ✓ If you are established outside the Union but caught by the Regulation, identify and appoint a representative in the Union (unless exempt)

## Core rules remain the same

- ✓ Review your existing compliance
- ✓ Work out if you are processing genetic or biometric information or information about criminal offences. If so, bring that processing into line with the new requirements of the Regulation

## Consent

- ✓ Review your existing processes to obtain consent to determine if they are valid under the Regulation
- ✓ Consider 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

## Data subjects' rights

- ✓ Consider if individuals are likely to exercise their new rights against you and what they mean for your business in practice
- ✓ Based on that analysis, set up processes to capture, record and act on those requests

## Privacy notices

- ✓ You will have to update your existing privacy notices.
- ✓ You should use the most effective way to inform individuals of your processing, such as layered or just-in-time notices.

## Accountability

- ✓ You will have to review and update your existing compliance policies. In some cases, you will need to create new policies.
- ✓ You will need to create and maintain a record of the processing you are carrying out (unless exempt).
- ✓ You should adapt your product development processes to include a privacy impact assessment, where necessary.

## Data protection officers

- ✓ Work out if you need to appoint a data protection officer. Even if you don't need to appoint a data protection officer, consider if you want to make a voluntary appointment
- ✓ 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
- ✓ Create a job specification for the role and appoint someone to that role

## Data security

- ✓ 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 Regulation

## Processors

- ✓ If you act as controller, update your contract templates to include the new 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 Regulation. What liability can and should you bear? What should properly be passed back to clients and customers? Do your terms 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?

## Transfers outside the Union

- ✓ You should review your current transfers and consider if they are justified now and will continue to be justified under the Regulation
- ✓ 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

## Sanctions

- ✓ You should review your current level of compliance and bring it up to the level required under the Regulation
- ✓ You should consider your overall attitude to risk and consider creating a risk assessment framework

# Glossary

---

**Board** means the European Data Protection Board (see *National regulators*)

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

**Data Protection Directive** means 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

**ePrivacy Directive** means Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector

**Individual** or **data subject**, means the living individual to whom the personal data relates (see *Existing concepts*)

**Lead supervisory authority** means the supervisory authority with primary competence over a business carrying out cross border processing (see *Consistency Mechanism - One stop shop*)

**Legitimate interests condition** means the processing condition set out in Article 6(1)(f) (see *Processing principles and 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?*)

**Network and Information Security Directive** means Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (see *Data security*)

**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*)

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

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

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

**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*)

**Public functions condition** means the processing condition set out in Article 6(1)(e) (see *Processing principles and conditions*)

**Sensitive 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 *Existing concepts*)

**Six general principles** means the general principles relating to the processing of personal data set out in Article 5 (see *Processing principles and conditions*)

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

# Contacts

---

## Brussels



**Tanguy Van Overstraeten**  
Tel: (+32) 2 501 94 05  
[tanguy.van\\_overstraeten@linklaters.com](mailto:tanguy.van_overstraeten@linklaters.com)

## Moscow



**Evgeny Ulumdzhev**  
Tel: (+7) 495 797 9797  
[evgeny.ulumdzhev@linklaters.com](mailto:evgeny.ulumdzhev@linklaters.com)

## Frankfurt



**Daniel Pauly**  
Tel: (+49) 69 710 03 570  
[daniel.pauly@linklaters.com](mailto:daniel.pauly@linklaters.com)

## Munich



**Konrad Berger**  
Tel: (+49) 89 418 08 168  
[konrad.berger@linklaters.com](mailto:konrad.berger@linklaters.com)

## Hong Kong



**Samantha Cornelius**  
Tel: (+852) 2901 5542  
[samantha.cornelius@linklaters.com](mailto:samantha.cornelius@linklaters.com)

## Paris



**Sonia Cissé**  
Tel: (+33) 1 56 43 57 29  
[sonia.cisse@linklaters.com](mailto:sonia.cisse@linklaters.com)

## Lisbon



**Carlos Pinto Correia**  
Tel: (+351) 21 864 00 15  
[carlos.correia@linklaters.com](mailto:carlos.correia@linklaters.com)

## Singapore



**Adrian Fisher**  
Tel: (+65) 6692 5856  
[adrian.fisher@linklaters.com](mailto:adrian.fisher@linklaters.com)

## London



**Richard Cumbley**  
Tel: (+44) 20 7456 4681  
[richard.cumbley@linklaters.com](mailto:richard.cumbley@linklaters.com)

## Stockholm



**Elisabet Lundgren**  
Tel: (+46) 8 665 67 77  
[elisabet.lundgren@linklaters.com](mailto:elisabet.lundgren@linklaters.com)

## Luxembourg



**Olivier Reisch**  
Tel: (+352) 2608 8294  
[olivier.reisch@linklaters.com](mailto:olivier.reisch@linklaters.com)

## Tokyo



**Mamiko Nagai**  
Tel: (+81) 3 6212 1232  
[mamiko.nagai@linklaters.com](mailto:mamiko.nagai@linklaters.com)

## Madrid



**Carmen Burgos**  
Tel: (+34) 91 399 6088  
[carmen.burgos@linklaters.com](mailto:carmen.burgos@linklaters.com)

## Warsaw



**Piotr Zawadzki**  
Tel: (+48) 22 526 5045  
[piotr.zawadzki@linklaters.com](mailto:piotr.zawadzki@linklaters.com)



---

Abu Dhabi | Amsterdam | Antwerp | Bangkok | Beijing | Berlin | Brisbane\* | Brussels | Cape Town\*\*\* | Delhi<sup>^</sup> | Dubai  
Düsseldorf | Frankfurt | Hanoi\* | Ho Chi Minh City\* | Hong Kong | Jakarta\*\* | Johannesburg\*\*\* | Lisbon | London  
Luxembourg | Madrid | Melbourne\* | Milan | Moscow | Mumbai<sup>^</sup> | Munich | New York | Paris | Perth\* | Port Moresby\*  
Rome | São Paulo | Seoul | Shanghai | Singapore | Stockholm | Sydney\* | Tokyo | Ulaanbaatar\* | Warsaw | Washington, D.C.

---

\* Office of integrated alliance partner Allens

\*\* Widyawan & Partners has an association with Linklaters LLP and Allens

\*\*\* Office of collaborative alliance partner Webber Wentzel

<sup>^</sup> Office of best friend firm TT&A

## linklaters.com

General editor: Peter Church

Updated October 2016.

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority.

The term partner in relation to Linklaters LLP is used to refer to a member of Linklaters LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications.

A list of the names of the members of Linklaters LLP and of the non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, One Silk Street, London EC2Y 8HQ, England or on [www.linklaters.com](http://www.linklaters.com) and such persons are either solicitors, registered foreign lawyers or European lawyers.

Please refer to [www.linklaters.com/regulation](http://www.linklaters.com/regulation) for important information on our regulatory position.