ALLEN & OVERY

Preparing for the General Data Protection Regulation

January 2018

Introduction

When the EU General Data Protection Regulation (GDPR) was finally agreed in April 2016, it seemed a long time until it would apply. However, as time races on, many companies are finding that there is a lot (for some, too much) to do.

The GDPR will apply automatically across all Member States from 25 May 2018. That includes the UK, notwithstanding Brexit. It will replace the 1995 EU Data Protection Directive.

The GDPR is an ambitious piece of legislation which took over four years to agree. One of the key aims was to create a harmonised approach to data protection across the EU, with bolstered rights for individuals in this age of rapid technological advances.

The GDPR sets a high standard for personal data protection throughout the EU, imposes a raft of new (sometimes onerous) obligations on those handling the data, and also provides for a much more punitive enforcement regime.

Given the scale of the task, many businesses have been working towards compliance for some time. However, various studies have shown that significant numbers of companies have not yet taken meaningful steps to prepare.

This article looks at some key areas of the GDPR to consider, drawing on our practical experience of implementing GDPR projects for a range of different organisations.

Contents

Foreword

Some commentators have suggested that the GDPR represents an evolution in data protection rather than a revolution. To some extent this may be true. Many of the changes introduced by the GDPR only cement existing good practice, such as privacy impact assessments, into the law or place on the statute book interpretations of the current law that have long been promoted by data protection authorities and, when tested, have been supported by the courts. One example is the new definition of personal data. This may seem to be much wider than the existing definition, referring as it does to location data and to online identifiers, but,in practice, the courts have already confirmed that, for example, IP addresses can be and often will be personal data. Furthermore the territorial reach of the EU data protection law has already been extended to some non-EU based data controllers by the decision of the CJEU in the well known Google Spain case.

The GDPR does though go much further than simply codifying existing good practice and incorporating legal developments. Extending the reach of EU law to businesses that offer their goods and services into the EU even though they may have no physical presence goes well beyond the Google Spain decision and might well be described as revolutionary.

Also the introduction of mandatory reporting of personal data breaches and mandatory data protection officers is likely to be considered revolutionary by many, not least by those Member States that, up to now, have not had any equivalent provisions in place . What is undoubtedly revolutionary though are the penalties that businesses will face if they get it wrong. Even in those few Member States that already have a system of fines in place, the level of the fines is nothing like the 4% of global turnover or EUR20 million now in prospect. And fines are not the only increased risk that businesses face. The GDPR brings new and enhanced rights for individuals and their expectations of how businesses treat their personal information are only going to get higher. Reputation and, with it, consumer trust and confidence will also be at increased risk. Put simply, the potential cost of getting data protection and privacy wrong is skyrocketing.

The GDPR also comes at a time when businesses are increasingly data driven. The volume of personal information that they are collecting and keeping is forever increasing with the information becoming, in many cases, a key business asset. This is an asset that can be exploited not just through increasingly sophisticated marketing operations but also through techniques such as "big data" analysis and the development of artificial intelligence. Data protection need not, and should not, stand in the way here.

On the contrary, businesses that understand their data protection obligations and seek to meet them in an intelligent way will be best placed to unlock the benefits of the personal data that they hold. Getting data protection right is not just a matter of legal compliance. It also makes sound business sense. So, whether evolutionary or revolutionary, the GDPR requires a step change for businesses in their management and delivery of personal data and privacy. Planning is required, priorities need to be set and resources allocated but no responsible business can afford to turn a blind eye to the GDPR's many requirements.

David Smith

Former Deputy Commissioner at the UK Information Commissioner's Office (ICO) and now special adviser to Allen & Overy

Who is subject to the GDPR?

The GDPR has a wider reach than laws implementing the Directive.

The GDPR applies to organisations (whether acting as data controller or data processor) that process personal data and are established in the EU. In some circumstances, it will also apply to organisations that process personal data and are established exclusively outside the EU.

There are three key triggers for the application of the Regulation.

The "establishment" test

If an organisation has an establishment in the EU, and processes personal data in the context of the activities of that establishment, it will be subject to the GDPR. It does not matter where the processing takes place (ie in the EU or not), whether it is undertaken by a third party (such as a subcontractor) or whether the personal data relates to data subjects resident or located in the EU.

This test focuses on having an "establishment" in the EU and processing being undertaken "in the context of the activities" of that establishment. The concept of an establishment has been interpreted broadly by the courts and is about exercising real and effective activity through stable arrangements, regardless of the legal form. Use of a local representative, website and address could be enough.

"There are three key triggers for the application of the Regulation, one familiar and two new."

The "goods and services" and "monitoring" tests

If a controller or processor is not established in the EU, the GDPR will also apply if it processes data about individuals who are in the EU and the processing relates to either:

- the **offering of goods or services** to data subjects who are in the EU; or
- **monitoring their behaviour**, where that behaviour takes place in the EU.

In each case, it is the location of the data subject that is important, not their nationality. The protection does not follow EU citizens if they travel.

To be **"offering goods and services"**, simply making available a website that can be accessed from within the EU is not enough. The controller or processor must somehow, demonstrably envisage offering services to data subjects in one or more Member States. The use of a local language or currency generally used in an EU country, or mentioning customers located in the EU, would suggest that the goods or services are being "offered" to people in the EU through that site.

"Monitoring" behaviour includes looking at whether natural persons are being tracked online and includes profiling techniques to predict personal preferences.

Organisations that do not have an establishment in the EU, but which are caught by the new tests, will have to appoint a representative in one of the relevant Member States. These organisations will need to determine how to achieve compliance of their GDPR-impacted activities.

Data controllers and data processors

The GDPR, unlike the Directive, applies to both controllers and processors. However, only a limited number of provisions of the GDPR apply directly to data processors. A greater number of provisions will indirectly impact data processors, as data controllers seek to pass on or delegate responsibilities of the controller to the processor. This is discussed further in "Data Processors".

Processing

As with existing legislation, **"processing"** is defined very widely and includes collecting, organising, storing, altering, retrieving, using, disclosing, combining and erasing personal data, amongst other activities.

Personal data

"Personal data" is any information relating to an identified or identifiable natural person. This might be by reference to an identifier such as a name, ID number, location data or online identifier, or by factors specific to them, such as their physical, genetic, economic or social identity.

While this definition might seem wider than that in the Directive, specifically including new elements such as online identifiers and genetic information is not really new.

The CJEU, for example, held in 2011 in *Scarlet Extended* that, from the perspective of an internet service provider (ISP), an IP address is personal data and in 2016 in *Patrick Brayer v Germany* clarified that even a dynamic IP address can constitute personal data when a company has the legal means to obtain additional information held by another party (such as an ISP) to identify the individual. Data protection laws in several Member States also specifically cover biometric or genetic data. However, by directly including online identifiers and genetic information in the definition of personal data, the GDPR clarifies this concept and harmonises diverging national approaches.

Exemptions

The GDPR does not apply in certain circumstances, such as processing for household activities.

Relevant articles & recitals

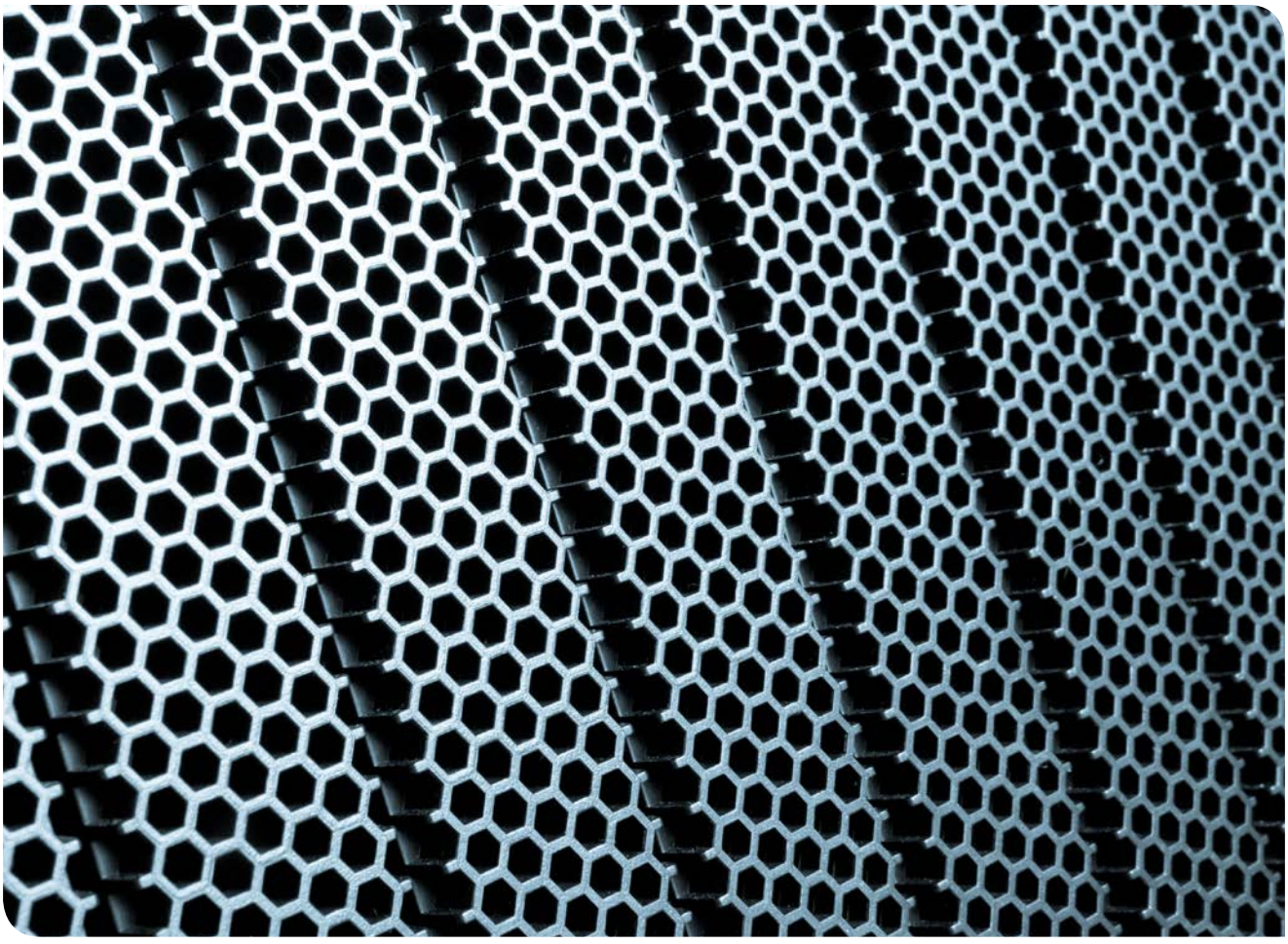
Article 3 – Territorial scope
Recitals 14 and 22-25

Article 4 – Definitions
Recitals 26-27 and 30

Impact

– For organisations outside the EU, identify whether there are circumstances in which the new "goods and services" or "monitoring" tests may apply. If identified, consider structural solutions (eg blocking EU visitors, or preventing cookies being placed on EU user devices), to avoid application of GDPR to non-EU entities, or extending GDPR compliance measures to relevant companies outside the EU.

– Data processors should look at how they will be affected and understand their new legal obligations as well as changes to the nature of their relationships with controllers.



When will it apply?

The GDPR will apply from 25 May 2018. As a Regulation it will apply in each Member State. Limited derogation, and certain other matters, will be set out in national laws which vary between Member States.

Although the GDPR will apply without the need to be specifically implemented into national law, most Member States will need to amend their national laws in order to address certain matters that are not addressed by the GDPR, such as legislation to deal with the supervisory authority's position, sector specific regulations or criminal offences. Member States also have the ability to introduce derogations (or as the European Commission prefers to call them "further specifications") in certain areas of the GDPR.

Member States are at various stages of considering possible derogation, and how they will deal in their local laws with repealing existing data protection legislation where necessary, perhaps keeping parts which are not inconsistent with the GDPR.

There are a number of areas where derogations are possible

Member States can introduce exemptions from the GDPR's transparency obligations and data subjects' rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is necessary and proportionate to safeguard, for example, national security and investigations into criminal offences.

Member States can also provide certain exemptions or derogations in relation to specific processing activities. These include processing of employee data and processing for archiving, scientific or historical research and statistical purposes.

Other areas where derogations are permitted include: supervisory authorities, further sanctions (eg criminal offences), processing special categories of personal data and criminal records, and third country transfers.

With such a wide range of areas where there is room for national rules to deviate, harmonisation across the EU will not be fully achieved.

Lawful grounds for processing

All processing of personal data must be based on lawful grounds.

This is not a new requirement, however under the GDPR it becomes much more important to understand and record the grounds on which personal data is processed.

In order to process personal data lawfully, a data controller (that is, the person that determines the purposes and means of the processing of personal data) must have at least one of a number of lawful grounds to do so. These lawful grounds may be established, for example, by:

– a legal obligation to process personal data;

– necessity of processing for the purposes of performing a contract with the data subject; or

– necessity for the purposes of "legitimate interests" pursued by the data controller or by a third party, provided not overridden by relevant fundamental rights and freedoms of data subjects.

A common misconception is that individual consent must always be obtained to process personal data lawfully.

The requirement to record the grounds for processing is particularly onerous and applies to all data controllers. This is discussed further in "Accountability".

Impact on data subject rights

The grounds for processing which a data controller relies upon determine the rights which are conferred by the GDPR on the data subject. For example, it may determine whether or not the individual has a right to object to processing of personal data or to data portability, or whether decisions can be made concerning a data subject using automated processing, including profiling.

Lawful grounds for processing under the GDPR

– The data subject has given consent to the processing for one or more specific purposes.

– Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

– Processing is necessary for compliance with a legal obligation to which the controller is subject.

– Processing is necessary in order to protect the vital interests of the data subject or another natural person.

– 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.

– 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.

Consent

A common misconception is that individual consent must be obtained to process personal data lawfully. In fact, consent is generally neither a prerequisite for lawful processing, nor is it always a cure for activities that would otherwise be considered unlawful. This remains the case under the GDPR.

Consent may be required for other reasons. For example, under the e-Privacy Directive (to be replaced by a proposed e-Privacy Regulation) the sending of unsolicited electronic marketing messages (ie by email or SMS) to a recipient generally requires the prior specific consent of that recipient.

Legitimate interests

The legitimate interests ground can be relied upon to the extent the processing of personal data is necessary for legitimate business reasons. It can no longer be relied upon by public authorities in discharging their function.

To rely on this condition a data controller should undertake an assessment as to whether or not the legitimate interests are overridden by the interests or rights and freedoms of the individual, which require protection of personal data. As such, factors such as the proportionality of data collection and processing, the reasonable expectations of individuals and their relationship with the data controller (eg customer versus prospective customer) must be taken into account. A data controller is expected to have carried out a "careful assessment" of the processing to ensure an appropriate balance is struck and, in the context of the much stricter sanctions regime under the GDPR, this becomes a decision with higher stakes.

A significant change under the GDPR is that if a data controller relies on a legitimate interest in order to provide lawful grounds for processing, this must be disclosed and explained to the individual data subject, as part of the fair processing information provided to the individual in a privacy notice. This will require organisations to look across the range of activities which are undertaken on the basis of a legitimate interest (as opposed to in reliance on consent or some other grounds) and to ensure that this is built into relevant privacy notices. We consider privacy notices in further detail in "Privacy notices".

Further processing

Where consent is not the ground chosen and a data controller wishes to use the data for another purpose, they must check whether the new purpose is "not incompatible" with original purpose of processing, considering for example links between the purposes, possible consequences and existence of safeguards. See further the section on "Purpose limitation" below.

Special categories of data

As under the Directive, the processing of special categories (which includes data about race, religion, sex life, health and political opinions) of data is prohibited except in limited circumstances, for example where "explicit" consent of the data subject has been obtained, where processing is necessary for certain legal matters or where processing is necessary for public health and in the public interest.

Furthermore, Member States are permitted to introduce additional conditions in relation to certain areas such as health, genetic and biometric data, and for the national identification number which could mean the rules become more restrictive over time and inconsistently applied across the Member States.

Data relating to criminal convictions and offences or related security measures which is processed based on one of the lawful grounds for processing can only be carried out under the control of an official authority or when authorised by EU or Member State law which provides for appropriate safeguards. This category of data is dealt with separately from the other "special categories".

Relevant articles & recitals

Article 6 – lawfulness of processing
Recitals 40-50, 112 and 171

Article 7 and 8 – conditions for consent
Recitals 32 and 42-43

Article 9 – processing special categories of personal data
Recitals 51-56

Article 10 – processing personal data relating to criminal convictions and offences

Article 87 – processing of the national identification number

Impact

– Implement a process (and associated documentation) to determine the grounds for processing personal data in relation to each processing activity the organisation undertakes.

– Revise privacy notices to reflect the basis for processing, including where the basis is legitimate interests, what those legitimate interests are.

– Implement a process (and associated documentation) for identifying circumstances in which the organisation may need to rely on consent to process personal data.

– Assess whether any processing carried out may be subject to derogations and therefore approached differently in different Member States.

Consent

Consent can serve a variety of purposes under the GDPR. However, it will be increasingly difficult, and potentially counterproductive, to rely on consent as a basis for processing.

Consent may provide a lawful ground for processing personal data. It may also provide a lawful ground for processing special categories of data. Or, it may be relied upon as a derogation from the restrictions on exporting data outside the EEA. It may also be necessary in order to send electronic marketing or to place cookies.

Although consent, if validly obtained, continues to serve these purposes, the requirements to obtain a valid consent have been tightened significantly under the GDPR.

There is now a raft of new requirements, alongside existing requirements that consent must always be freely given, specific and informed, which must be satisfied in order to obtain a valid consent. This will make consent much harder to obtain and maintain, and will require a different approach to existing market practice.

What are the requirements for a valid consent under the GDPR?

Consent must be a freely given, specific, informed and unambiguous indication of the individual's wishes. In addition, the consent must satisfy the following requirements:

- The request for consent must be in an **intelligible and easily accessible** form, in clear and plain language.
- The request for consent must be **clearly distinguishable** from other matters.
- The consent must consist of a **clear affirmative action**.
- If the personal data will be processed for multiple purposes, consent must be **given separately for each purpose**.
- Consent will not be valid if the individual does not have a **genuine free choice** or if there is a detriment should they refuse or withdraw consent.
- Consent may be invalid if there is a clear **imbalance of power** between the controller and individual.
- Consent will be presumed to be invalid if it is a **condition of performance of a contract** despite not being necessary for such performance.
- Consent must be able to be withdrawn at any time and **should be as easy to withdraw as it is to give**. The individual must be informed of their right to withdraw at the time of giving consent.

As consent must be obtained by way of a clear and affirmative action, data controllers can no longer rely on inferred consent. Inactivity, pre-ticked boxes or silence are not enough, but consent may be indicated through a course of conduct.

The GDPR clarifies that a clear and affirmative action may include ticking a box to signify consent when visiting a website or choosing clear technical settings.

Consent can be withdrawn

An existing limitation of consent as a basis for processing, which remains under the GDPR, is that if the consent is relied upon as the sole basis for processing then as soon as the consent is withdrawn a data controller will be required to cease that processing, which could require it to undertake a purge of the relevant data if it has no other lawful basis for processing. Implementing systems and processes to manage repercussions of withdrawal of consent could require significant investment.

There is no 'grandfathering' of consents obtained before the GDPR applies

Where consent has been given, it will continue to be valid under the GDPR only to the extent it meets the more stringent requirements of the GDPR. This could mean that consent needs to be obtained again where those requirements have not been met.

For example, as many marketing databases may have relied on pre-ticked boxes or other implicit consent to processing in the past, and may have bundled consent to processing along with other terms and conditions or generic privacy notices, organisations may find that the data held in their existing databases is no longer usable for some marketing purposes.

As noted above, consent continues to be required in order to send direct marketing to consumers by email or SMS, unless there is an existing relationship with the individual which enables you to fall within the so-called "soft opt-in" exemption.

The requirements in relation to direct marketing are set out in the e-Privacy Directive, not the GDPR (which simply contains a right to object to direct marketing), although concepts from the GDPR, such as the requirements in relation to validity of consent, do apply, so the tougher requirements under the GDPR will have an effect on these activities. The e-Privacy Directive is in the process of being replaced by a proposed Regulation .

Relevant articles & recitals

Article 4(11) – Definitions (consent)
Recitals 32-33 and 42-43

Article 6(1) – Lawfulness of processing (consent)
Recitals 40 and 171

Article 7 – Conditions for consent
Recitals 32 and 42-43

Article 8 – Conditions applicable to child's consent in relation to information society services
Recital 38

Article 9(2)(a) – Processing of special categories of personal data (consent)
Recital 51

Article 49(1)(a) – Transfer to third countries; Derogations for specific situations: explicit consent
Recital 111

Impact

– Implement a process for identifying circumstances in which the organisation may need to rely on consent to process personal data.

– Where it is necessary to rely on consent, implement a process to maintain a written record of all consents the organisation has obtained in relation to each processing activity the organisation undertakes, to demonstrate that consent has been validly given in each case.

– Implement a process to manage consequences of withdrawal of consent, where consent is relied on as grounds for processing personal data (ie to prevent further processing).

– Review forms of consent to ensure they meet the requirements for a valid consent under the GDPR and provide the maximum possible flexibility to exploit personal data for the required purposes.

– Carry out an audit of existing data sets to establish to what extent valid consent has been obtained. Establish whether it will be necessary to seek fresh consent in order to meet the requirements of the GDPR. Organisations will need to consider whether or not it is viable to obtain fresh consent, as it may be difficult to satisfy the new requirements and the exercise could be onerous.

– Ensure data subjects are given a genuine choice as to whether to provide consent, and are free to withdraw consent without detriment (eg consent is not a condition to performance of a contract).

– Ensure that consent is distinguished from other matters (eg not incorporated into another document such as terms and conditions or an employment contract).

– Ensure that the data subject is aware at least of the identity of the data controller and the purpose of processing before they are asked to provide consent and ensure that the consent is informed (eg through providing a privacy notice);

– Ensure consent is written in clear and plain language so it is clear what the data subject is being asked to consent to; that the that the consent is provided by a clear affirmative act, such as ticking a box; and in respect of special categories of data, that the consent is explicit (eg the organisation explicitly uses the term "consent" in the form of consent the data subject is asked to provide).

Privacy notices

Data controllers must be more transparent with data subjects about their processing activities.

Individual data subjects must have information made available to them about the manner in which, and the purposes for which, their personal data is processed.

That information must be concise, transparent, intelligible and easily accessible. However, at the same time the "shopping list" of information that must be included in a privacy notice is expanded significantly under the GDPR.

As with forms of consent, existing privacy notices will have to be looked at to check whether these more detailed requirements are met.

There is no grandfathering of existing notices which do not meet GDPR requirements

Fresh privacy notices may need to be made available. Existing notices may need to be revised for future use.

How to provide a valid privacy notice:

Whether data is obtained directly from the data subject or via third parties a privacy notice must specify (among other things):

- The identity and contact details of the controller, and of their representative (if any).
- The contact details of the controller's data protection officer.
- The purposes and legal basis for the processing – and where legitimate interests are relied upon, those interests.
- The right to withdraw consent (if consent is the basis for the processing).
- The categories of personal data processed. (only where collected from the 3rd party and not directly from the data subject).
- The recipients or categories of recipients of the personal data (eg third party partners or vendors).
- The source of the personal data, including use of public sources, only where collected from third party and not directly from the data subject.*
- Details of any intended transfer outside the EU, including details of any safeguards relied upon.
- The period for which the data will be stored or criteria used to determine that period.
- Details of the individual's rights, including the right to complain to a supervisory authority.
- Details of any automated decision making.

*Only if data is obtained from a third party.

There is a fundamental challenge in designing privacy notices. On the one hand, the data controller must communicate with the individual in a clear and intelligible manner, but, on the other hand, it must communicate quite detailed and forward-looking information about its data processing activities.

There is also a balance to be struck when providing this specific information between accurately describing processing activities and future-proofing a privacy notice. Future-proofing may involve, for example, writing the privacy notice in such a way that it allows the data controller the greatest flexibility to use personal data as required, including for purposes which were not specifically known at the time of data collection, while still complying with the requirements of the GDPR.

It is likely that any business operating complex systems will find it difficult to include all the information required in a privacy notice, without changes to existing arrangements. Some of the requirements are also fairly onerous.

The requirement to specify the period for which data will be stored, or if that is not possible the criteria used to determine that period, may be a particular challenge, and may require a controller to look at other solutions such as anonymisation of data after a defined period.

The information required may be provided in combination with standardised icons, though these are not proving popular so far.

The information must be provided by the data controller at the time the data is obtained where it is collected directly from the data subject.

Relevant articles & recitals

Article 12 – Transparent information, communication and modalities for the exercise of rights of the data subject
Recitals 11, 58-60

Article 13 – Information to be provided where personal data are collected from the data subject
Recitals 11 and 61-62

Article 14 – Information to be provided where personal data have not been obtained from the data subject
Recitals 11 and 62

Impact

– Review privacy notices to ensure all required information is included.

– Review privacy notices for readability. Consider undertaking a "plain English" review.

– Consider how privacy notices are communicated. Balance the need to provide detailed information with ensuring that it is clear. For example, consider layering of privacy notices, so as to draw only unexpected or otherwise key information to the individual's attention, whilst allowing them to find further detail where desired.

– Consider when to give a privacy notice – "just in time" notices may be particularly effective.

– Consider how privacy notices may be adapted in the future to incorporate standardised icons or similar techniques.

– Implement a process to ensure that privacy notices are recorded and retained.

Purpose limitation

Personal data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

There is some room to expand the purposes for which data is processed beyond those which were contemplated at the time of collection, but any further use must not be "incompatible".

The GDPR states that the controller must consider whether a further purpose is compatible with the purpose for which the data was originally collected. If the controller determines that the purposes are incompatible, they may need to seek consent or not undertake the proposed processing. Things to take into account include any link between that purpose and the intended purpose, the context in which the personal data was collected, the reasonable expectations of the data subject based on their relationship with the data controller, the nature of the personal data, the possible consequences of the intended processing and the existence of appropriate safeguards.

Many data management systems will draw upon a range of sources of personal data. In doing so, organisations must consider whether there is any expansion of the purposes for which data was originally collected. It is important to be mindful of the need to restrict the use of the data to the purpose for which it was collected, although the reality is that detailed records of the purposes for which particular data was originally collected may not be held. In these circumstances, it may be necessary to undertake a risk assessment and consider if safeguards can be implemented to reduce risk to the rights and freedoms of individuals.

Relevant articles & recitals

Article 6(4) – Further processing
Recital 50

Impact

– If considering using personal data for further purposes, assess whether those purposes are incompatible with the original purpose for which data was collected.

– Review privacy notices and forms of consent to ensure the purposes of processing are accurately reflected. Consider whether the notice strikes the right balance between flexibility and the need to be specific.

– Implement appropriate processes and written controls, to ensure proper control over use of information for further purposes.

Rights of data subjects

The GDPR has enhanced, and extended, the rights of data subjects.

The GDPR introduces some new rights – such as the right to portability – and codifies the much heralded "right to be forgotten", as well as making changes to rights that exist under the Directive.

There is a short response time. The data controller must respond within a month, with a possibility to extend this period for a further two months for particularly complex requests.

There is a limited ability to claw back costs in limited cases, although information must be provided free of charge unless the request is "manifestly unfounded or excessive".

Member States may restrict the scope of the obligations and rights to safeguard, for example for reasons of national security, defence, public security, criminal investigations or other important objectives of general public interest. This may lead to a divergence of rights across different Member States in certain areas of national interest.

Rights of access

This right to make a data subject access request (often called a "DSAR") is a right for a data subject to obtain confirmation from a data controller as to whether personal data about them is being processed, as well as a copy of that personal data. This right also entitles a data subject to obtain certain available information such as where the personal data was collected from and how it is processed, for instance whether the controller is using it for profiling purposes. It should be easily exercisable at reasonable intervals.

This right, which already exists under the Directive, has proved burdensome on companies in some jurisdictions and is often criticised as being used as a fishing expedition or pre-litigation disclosure tactic.

There are strategies which are currently used for paring back the scope of the DSAR, such as by excluding non-personal data, relying on the narrow exemption that applies to privileged material, or arguing that complying entails disproportionate effort. However these are risky and not supported by all regulators. It is not yet clear whether these strategies will work under the GDPR as it is left to Member States to introduce exemptions.

Right to rectification

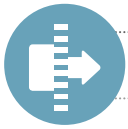
This is a right for data subjects to obtain, without undue delay, rectification of inaccurate personal data about themselves. Depending on the purposes of the processing, data subjects may also have a right to have incomplete data completed.

Right to erasure

Also called the "right to be forgotten", this entitles data subjects to have their personal data erased without undue delay. Following the well-publicised Court of Justice of the EU (CJEU) decision in the case of *Google Spain* where Google had to remove links to certain newspaper articles from listed Google search results of a Spanish resident's name (the articles referred to his historic financial problems), some companies have been inundated with requests for unpalatable data about individuals to be erased.

The expectations of data subjects do not necessarily match their actual rights and this is a good example. Despite receiving a request for erasure under this right, data controllers may continue to process the data if it is still necessary in relation to the purposes for which it was lawfully collected and processed and they are not relying on withdrawn consent.

There are various other exemptions, for example for processing which is necessary for certain reasons of public interest in the areas of public health, and for scientific or historical research purposes where the right is likely to render impossible or seriously impair the achievement of the relevant objectives of the processing (subject to appropriate safeguards). This latter exemption is one of the areas where Member States may derogate.



Rights to restrict processing

Data subjects have the right to obtain restriction of processing in certain circumstances. For example, if a data subject contests the accuracy of the personal data, processing may be restricted while its accuracy is being verified. This right also applies where the processing is unlawful but the data subject doesn't want it to be erased, or where the controller doesn't need the data but it is still required by the data subject for the establishment, exercise or defence of legal claims. During the restriction the personal data shall (except for storage) only be processed with consent or in certain other circumstances.

Right to object

This applies when the ground for lawful processing is based on it being necessary for performing tasks carried out in the public interest or in the exercise of official authority vested in the controller. It also applies where the ground is based on legitimate interests, including profiling based on those grounds. Data subjects can object based on their particular situation at any time.

The data controller should stop processing unless it can demonstrate compelling legitimate grounds which override the interests of the data subject, or for the establishment, exercise or defence of legal claims. There is also a right to object to direct marketing (see further details in "Automated processing and profiling").

Right to data portability

Individuals can ask to receive personal data that they have provided to a controller in a structured, commonly used and machine-readable format so that it can be easily transferred to another data controller/service. The idea is to give the data subject more control for example by facilitating switching between service providers.

In order to fall under the scope of data portability, processing operations must be based on either the data subject's consent or on a contract to which the data subject is a party, and the processing must be carried out by automated means.

This obligation does not impose a right to retain personal data for longer than necessary simply for a potential future request.

The Article 29 Working Party released guidelines at the end of 2016 on how to interpret and implement this right to data portability. They state that the right covers data provided actively and knowingly by the data subject as well as personal data generated by his or her activity. The European Commission has expressed concern that including "generated" data goes beyond what was agreed in the GDPR legislative process and this point is therefore controversial.

The guidance specifies that data controllers that outsource data processing or process data jointly with other controllers must have clear contractual arrangements to allocate responsibilities regarding the handling of data portability requests.

Relevant articles & recitals

Article 12 – Communication and modalities for the exercise of rights
Recital 11, 59

Article 15 – Right of access by the data subject
Recitals 59, 63-64 and 73

Article 16 – Right to rectification
Recitals 59, 65 and 73

Article 17 – Right to erasure ('right to be forgotten')
Recitals 59, 65-66 and 73

Articles 18 – Right to restriction of processing
Recitals 67 and 73

Article 19 - Notification of rectification, erasure or restriction
Recital 11, 59

Article 20 – Right to data portability
Recitals 60 and 68

Article 21 – Right to object
Recitals 69-70

Article 22 – Automated individual decision making, including profiling
Recitals 60 and 71-72

Article 23 – Restrictions
Recital 73

Impact

– Implement clear and robust processes to respond to the exercise of data subject rights. These should be proportionate to the volume of requests expected to be received.

– Implement a process to enable verification of the identity of the individual making a request.

– Implement policies regarding how requests will be dealt with (eg will the organisation sometimes seek to recover costs, where chargeable?).

– Implement a process to inform third parties about restriction requests (other than where this is impossible or involves disproportionate effort).

– Implement systems to maintain a copy of personal data in a structured, commonly used and machine readable format, where necessary for the exercise of the right of portability.

– Mechanisms may need to be put in place to enable data subjects to make requests/objections, eg through a portal. The Recitals to the GDPR suggest that the controller should provide electronic means, especially whenever the data are processed by electronic means.

Accountability

The GDPR imposes onerous accountability obligations on data controllers.

Notable among these, a data controller will be required:

– to maintain records of all processing activities under its responsibility – a daunting undertaking which should not be underestimated, but equally should not be over-engineered;

– to conduct data protection impact assessments for more risky processing, including to identify where they are required in the first place – many organisations will implement some level of DPIA by default into their processes;

– to implement data protection by design and by default (see section on "Privacy by Design"); and

– to notify certain data breaches (see section on "Data security and data breach notification").

It may also be necessary to appoint a data protection officer.

It will be necessary to demonstrate to supervisory authorities the basis on which personal data is processed, and more generally how the requirements of the GDPR are met.

An on-going audit, quality assurance and improvement programme is likely to be required to monitor and report on privacy compliance within the organisation.

Keeping records

The duty to keep records is particularly onerous. These records will need to be made available to the supervisory authority on request. In the context of legacy systems, configuring systems to maintain records of all the information required may be extremely challenging. A number of technological solutions to assist companies with this challenge have emerged on the market.

A controller must keep a record of the following information:

– The controller's name and contact details, and (where applicable) details of any joint controllers, and the controller's representatives or data protection officers.

– The purposes of the processing.

– A description of the categories of data subjects and 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.

– Envisaged retention periods for different categories of personal data (where possible).

– A general description of the security measures in place (where possible).

A processor must:

– Maintain a record of all categories of processing activities carried out on behalf of a controller, including transfers to third countries and security measures taken.

Data protection impact assessments

If engaging in high-risk processing, it will be necessary to conduct a data protection impact assessment (DPIA). This would be required, for example, when processing special categories of personal data on a large scale, or using new technologies or collating systematic and extensive profiles. Further detailed guidance has been provided by the Article 29 Working Party. Helpfully, a single assessment may address a similar set of processing operations.

A particular challenge for complex organisations will be to identify where a DPIA is required without an unduly onerous assessment process. This will include asking questions of a business process or IT asset owner to identify key information about the processing activities. Some of the information may be collected in any event to maintain the written record of processing.

Many organisations are turning to technology tools to assist with undertaking DPIAs in a business friendly, semi automated manner. It may be necessary to consult the supervisory authority prior to processing if risks identified in a data protection impact assessment are high and cannot be effectively mitigated.

Data protection officers

Many companies will be required to appoint a data protection officer (DPO). This is required, for example, if the core activities of the controller or processor consist of processing which, by its nature, scope or purposes, requires regular and systematic monitoring of data subjects on a large scale, or where the core activities involve large scale processing of special categories of data and data relating to criminal convictions and offences.

The DPO may be employed or engaged under a service contract. A group of undertakings may appoint a single DPO (conditional on accessibility by all).

The DPO will need sufficient expert knowledge. This will depend on the processing activities for which the officer has oversight. They may fulfil other tasks as long as there is no conflict of interest. The DPO must be involved in all issues which relate to the protection of personal data and various specific tasks which are expected of them are set out in the GDPR. They must report directly to the highest management levels.

The Article 29 Working Party guidance on DPOs makes it clear that where a business decides to appoint a DPO voluntarily, they will still be subject to the same requirements as mandatory DPOs, and that other data protection professionals should have different titles. Where a company decides that it is not required to appoint a DPO, the Article 29 Working Party recommends documenting the reason for the decision (unless it is obvious).

The contact details of the DPO must be published by the data controller or processor who must also communicate those contact details to the supervisory authority.

As organisations start to look at who to appoint as a DPO, it is becoming clear that this is a role which straddles many areas of a business including legal, security, compliance and risk. The DPO will need to be comfortable presenting to senior management on data protection issues, and cooperating with the supervisory authority.

Relevant articles & recitals

Article 30 – Records of processing activities
Recital 82

Article 35 – Data protection impact assessment
Recitals 75-77, 84 and 89-94

Article 36 – DPIAs: Prior consultation
Recitals 94-96

Article 37– Designation of the data protection officer

Article 38 – Position of the data protection officer

Article 39 – Tasks of the data protection officer

Recital 97

Impact

– Generate relevant records for existing processing activities.

– Implement systems and processes to enable your organisation to capture and store relevant records.

– Consider in what circumstances your organisation will undertake data protection impact assessments and how these will be reviewed over time. Implement a process and relevant documentation and systems to put this into practice.

– Establish if your organisation has a duty to appoint a DPO and, if so, consider what role the DPO will have.

Privacy by design

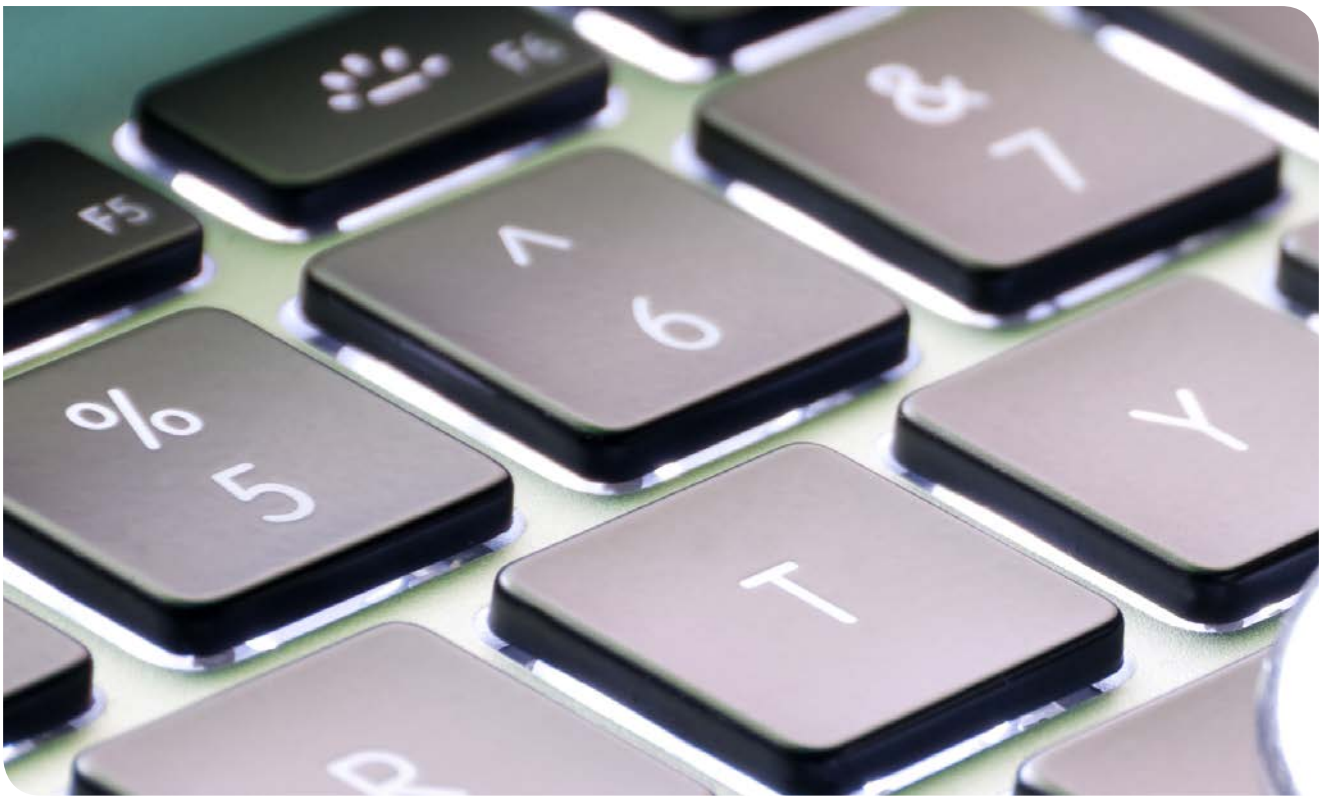
The GDPR requires that you implement privacy by design.

Privacy by design is an approach to protecting privacy in the creation of systems (technologies, business practices and physical design of networked infrastructures) that focuses on privacy upfront by embedding it into the architecture from the beginning.

Privacy by design means implementing appropriate measures both when determining the means for processing and at the time of the processing itself, which implement the data protection principles (such as data minimisation). When thinking about privacy by design, an organisation should take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks to individuals.

This obligation requires considering privacy at the beginning of undertaking new activities involving personal data processing, or when implementing new or modified data management systems.

In addition to privacy by design, the GDPR also requires data controllers to implement privacy by default which again addresses issues of data minimisation. Under this principle, organisations should, for instance, ensure that personal data are not by default (ie without the intervention of the data subject) made accessible to an indefinite number of people. It follows that social media providers should not by default set up profiles as public.



Relevant articles & recitals

Article 25 – Data protection by design and by default
Recitals 74-78 and 108

Impact

– Implement a process or a policy, to implement appropriate technical and organisational measures to implement data protection principles, such as data minimisation.

– Think about privacy when:

  – creating new products, applications and services.

  – building a website - how are you collecting data and what information do you provide to data strategies about your data collection? Are you using third party scripts such as social media buttons, advertising or comment platforms which may be collecting additional data or setting cookies?

  – choosing third party processors, does the processor have a reputation for security and are they willing to help you to comply with your data protection obligations?

  – developing new business strategies – eg are the strategies you are creating compatible with data privacy? Are you collecting too much data? Are you using the data for the right purposes?

– Implement a process to implement appropriate technical and organisational measures to ensure that, by default, only personal data which is necessary for each specific purpose of processing is processed.

Automated processing and profiling

A data subject has the right not to be subject to automated decisions including those based on profiling if the decision produces legal effects concerning, or otherwise similarly significantly affects, that data subject.

"Profiling" (as defined in the GDPR) refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Examples of the use of profiling in the context of automated decisions include the automated refusal of an online credit application, or e-recruiting practices without any human intervention.

Individuals have the right not to be subject to decisions based solely on automated processing (including profiling) which produces legal effects concerning them or which similarly significantly affects them other than in certain limited situations. The Article 29 Working Party sees this as a prohibition on fully automated individual decision making in these circumstances. Others argue that this is a right for the individual to object. The exceptions to this rule include where the individual has given explicit consent, where making of such decisions is authorised by EU or Member State law, or where it is necessary for entry into or performance of a contract between the data subject and the controller.

Even in these cases, the controller is required to provide certain protections for the data subject to safeguard their rights, freedoms and legitimate interests with at least the right to obtain human intervention, express their views and contest the decision.

As already touched upon above, the GDPR requires data controllers to notify individuals about the existence of automated decision-making including profiling. Data controllers must, in certain situations, explain the logic involved and the significant and envisaged consequences of the profiling for the data subject. This is becoming increasingly relevant for companies seeking ways to explore the benefits of AI, machine learning and big data analysis for business application, for example when evaluating risks for car insurance pricing, credit scoring or recruitment.

Relevant articles & recitals

Article 4 – Definitions ('profiling')

Article 22 – Automated individual decision-making, including profiling

Recitals 60, 68 and 71-73

Impact

– Identify whether you make automated decisions which produce legal effects concerning individuals or similarly significantly affect individuals.

– Implement a process to allow individuals to request human intervention in decisions based on automated processing, to express their views and to contest the automated decision, noting that there are some exceptions.

– Find ways to describe, in clear and meaningful terms, the logic involved and the significance and the consequences of the processing for the individual. Consider which technical and organisational approaches to algorithmic transparency should be used for processing.

Data security and data breach notification

Data controllers and data processors are now required to notify certain data breaches.

Where there is a breach of personal data, such as unauthorised access to, or loss of, data, various obligations to notify may arise.

Notification of the competent supervisory authority

This must be done without undue delay and, where feasible, within 72 hours of becoming aware of the breach. However, the obligation does not apply if the breach is unlikely to result in a risk to the rights and freedoms of individuals. If the controller does not notify within this time period, it must explain the reason for the delay. The notification must at least describe the nature of the breach, the categories and approximate number of data subjects and records concerned, details of the DPO or other contact point, the likely consequences and the measures being or proposed to be taken.

All data breaches must be documented including the effects and any remedial action taken.

Notification of data subjects

This must be done without undue delay if the data breach is likely to result in a high risk to the rights and freedoms of individuals. This notification must describe the breach clearly and provide certain other information. Notification may not be required, for example, if the data has been securely encrypted and access to the encryption key has not been compromised.

A public communication may be sufficient if notification on an individual basis would involve disproportionate effort.

Data processors must notify the controller

By contrast to the Directive, a data processor also has a direct obligation under GDPR. Data processors must notify the controller without undue delay after becoming aware of a personal data breach.

These new requirements formalise the existing recommendations of supervisory authorities like the ICO. They also harmonise the requirements across Member States.

This obligation sits alongside other requirements to notify security breaches

Some sector specific legislation, for example, contains an obligation to notify in certain circumstances. Good examples are the financial services sector and the telecoms sector. Under the e-Privacy Directive, for instance, service providers (eg telecoms providers or internet service providers) have an obligation to notify personal data breaches to the relevant supervisory authority within 24 hours of detection, where feasible. In some Member States, the relevant supervisory authority will also be the data protection authority. They must also notify the subscribers or users without unnecessary delay if the breach is likely to affect their personal data or privacy. The proposed draft ePrivacy Regulation and Telecoms Code suggest that these obligations will remain in some form.

In addition, the EU NIS Directive on network and information security contains an obligation on those companies to which it applies (such as those providing essential services in the Member State) to notify certain security breaches. This notification could be to a different supervisory authority than that overseeing the GDPR in some Member States and applies to all security incidents even if no personal data is involved.

Relevant articles & recitals

Article 30 – Records of processing activities
Recital 82

Article 32 – Security of processing
Recital 83

Article 33 – Notification of a personal data breach to the supervisory authority
Recital 85, 87-88

Article 34 – Communication of personal data breach to the data subject
Recitals 86-88

Impact

– Update or create internal processes for identifying and reacting to a personal data breach, including creating the relevant documentation, within the timescales expected by the GDPR.

– Create a written record of the technical and organisational measures in place, as part of the records of processing.

– Implement a process to maintain a written record of data breaches, including remediation actions taken in response.

– Review your agreements with third party suppliers to ensure they have a clear obligation to notify you where required.

– Check what your insurance policies cover in the event of a personal data breach.

– Implement a process to ensure that security measures are regularly tested and kept up to date.

– Implement a process to anonymise or pseudonymise data where applicable.

– Implement a process to identify high risk processing activities.

– Create a process and team to deal with the aftermath of an incident. Organisations should ensure a public relations communications plan is in place and appoint any external specialists ahead of time.

– Regularly test your plan by simulated incidents.

– Ensure you take into account breach reporting requirements in other jurisdictions (including outside the EU) and sector specific requirements.

Data processors

Under the GDPR, data processors have direct obligations for the first time.

Data processors are those who process personal data on behalf of a data controller. Under the Directive and its implementing legislation in most Member States, data processors do not have direct obligations. As a consequence, processors have been subject only to contractual requirements regarding data processing which are set out in their agreements with customers.

In contrast, the GDPR imposes a number of direct obligations on data processors. This will alter in some significant respects the dynamic of the relationship between controllers and processors.

This will be a major change for the suppliers of services in particular. For example, data processors may find themselves jointly and severally liable, together with the data controller, for compensation claims made by individuals.

The obligation on data controllers to enter into a binding contract with any data processor, containing certain minimum provisions, remains. However, the list of required provisions has become more extensive. As such, both existing contracts with suppliers and new contracts should be reviewed to ensure they meet GDPR requirements.

In addition, under the GDPR, data controllers may only engage data processors that provide sufficient guarantees to implement technical and organisational measures to ensure that the relevant processing will comply with the GDPR and ensures the protection of rights of individuals.

This effectively introduces the indirect obligation for data processors to ensure their processing is compliant with the GDPR and appears to be a wider obligation than in the Directive which focuses on sufficient guarantees around security of processing (ie protecting personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing).

Set against all of this is the much tougher enforcement regime (see "Enforcement" section). This will fundamentally alter the risk profile of controller-processor and controller-controller relationships. Parties, and their insurers, will be focused on ensuring exposure to data protection risk and liability is appropriately managed, which will lead to renegotiation of the liability provisions in many commercial relationships.

What needs to be in a data processing agreement?

Each agreement should contain a description of the data processing activities. It should ensure that the processor:

- only processes personal data on the data controller's documented instructions unless required to do so by Member State or EU Law (in which case it must inform the controller of that requirement);
- ensures that any people (eg employees) it uses to process personal data are under appropriate obligations of confidentiality;
- does not disclose personal data to anyone else without the data controller's consent;
- has appropriate security measures in place to protect personal data, in accordance with applicable data protection laws;
- does not engage sub-processors without prior authorisation and makes sure that the same obligations are flowed down to any subcontractors it does use to process personal data;
- assists the data controller in relation to the data controller's obligations to comply with applicable data protection laws, including in relation to reporting security breaches, undertaking privacy impact assessments and responding to requests from data subjects;
- deletes or returns personal data when it is no longer required (eg when the services and/or contract terminates or expires); and
- makes available to the data controller any information necessary to demonstrate its compliance with these obligations including allowing, and contributing to, audits and inspections.

Relevant articles & recitals

Article 28 – Processor
Recital 81

Article 29 – Processing under the authority of the controller or processor

Article 30 – Records of processing activities
Recital 82

Article 31 – Cooperation with supervisory authority
Recital 82

Article 32 – Security of processing
Recital 83

Article 33 – Notification of a personal data breach to the supervisory authority
Article 82 – Right to compensation and liability
Recital 146

Impact

- Review existing contracts with data processors (eg suppliers) and associated processes to verify that the contracts contain at least the minimum provisions required under the GDPR. Establish a remediation process to amend contracts where required, by May 2018.
- If you use a third party processor, look into their roadmap for GDPR compliance. What steps are they taking to meet their obligations under GDPR, or to enable you to meet yours?
- Update or create internal processes for verifying that new third parties processing personal data on your behalf are compliant with the GDPR; assess and verify this periodically for existing contractual relationships.

Data transfers to "third countries"

The data transfers regime remains largely the same, with increased recognition of BCRs.

There are a number of mechanisms set out in the Directive which can be relied on to transfer personal data lawfully outside the EEA. The "toolkit of available mechanisms" under the GDPR is essentially the same:

Transfers to "adequate" countries

The European Commission is able to determine that a country (or specific sector) offers an adequate level of protection for data transfers. The CJEU made it clear in the *Schrems* case against Facebook (which looked at the EU-U.S. Safe Harbor regime) that the test should be one of "essential equivalence" and a carbon copy of EU law is not required. The adequacy status of countries which have been granted adequacy under the Directive does not change under the GDPR but it will be subject to review. This will include Argentina, Canada (PIPEDA), U.S. (Privacy Shield for those organisations who self-certify), Switzerland, Israel and New Zealand. Japan and South Korea are in the process of obtaining adequacy status too.

The advantage of transferring personal data to a country that has been found to be 'adequate' is that the transfer can take place as if the country was within the EU.

Some form of adequacy finding looks likely to be a preferred route for the UK post-Brexit.

Transfers subject to appropriate safeguards

BCRs

Cross border data transfers within a corporate group under Binding Corporate Rules have been recognised by the Article 29 Working Party for some years but have been formally included as a transfer mechanism in the GDPR.The GDPR provides one set of standards applicable to BCRs. In practice there are two types of BCRs. BCRs for Controllers regulate personal data transfers by the organisation as data controller within the same company group. BCRs for Processors are used for international transfers of personal data that is originally processed by a processor on behalf of an EU controller and that are sub-processed within the processor's organisation. While some new requirements for BCRs are introduced by the GDPR, the full list of requirements which apply to each type of BCRs is still considerably shorter than the detailed criteria established by the Article 29 Working Party. However, the European Commission may establish additional requirements and the European Data Protection Board may issue guidelines, recommendations and further necessary requirements. In practice this might mean that the EPDB will uphold the Article 29 Working Party opinions on BCRs, with a risk of re-introducing administrative requirements that are simplified by the GDPR. In the absence of official clarification, companies that intend to adopt BCRs may wish to seek advice from their lead supervisory authority.

Companies that already have BCRs should be looking to ensure that they are consistent with the requirements of the GDPR and will almost certainly need to prepare for re-submitting an application for new approval.

Until now, BCRs have been limited to arrangements among entities of the same corporate group. Under the GDPR, BCRs can be used by a group of enterprises that are engaged in joint economic activity, but are not necessarily part of the same corporate group.

The GDPR leaves several practical questions open such as the criteria to be used to determine whether businesses meet this requirement.

It also looks likely that the rules for selecting a lead authority for BCR authorisation, at least for group companies, will probably become less flexible under the new One Stop Shop regime.

Standard Contractual Clauses approved by the Commission

Standard clauses adopted by the European Commission (Model Clauses) are a commonly used mechanism for legitimising transfers of personal data to third countries. They comprise standard agreements.

While this option remains in the GDPR, the data protection community is closely watching a case brought by Max Schrems against Facebook in Ireland which challenges this mechanism. Given that various questions have been referred to the CJEU, there is a risk that use of Model Clauses, at least in certain scenarios, may be declared unlawful in the same way the CJEU declared the Safe Harbor regime for transferring data to the U.S. unlawful. As many companies rely on this mechanism, its removal, even for certain transfers, would cause substantial upheaval and uncertainty.

Standard Contractual Clauses adopted by a supervisory authority

A supervisory authority may also adopt Standard Contractual Clauses. These must be approved by the Commission.

There is a welcome removal of the need for prior authorisation for transfers based on approved safeguards such as Commission or DPA approved Standard Contractual Clauses. This requirement was imposed by some Member States in implementing the Directive but has been expressly excluded in the GDPR.

An approved code of conduct

The GDPR encourages the implementation of Codes of Conduct to help apply the Regulation, taking into account the needs of different processing sectors and smaller enterprises. One of the areas suggested for the use of Codes is the transfer of data to third countries, where the approved codes can provide appropriate safeguards required by the GDPR.

Associations and other bodies representing categories of controllers or processors may prepare codes. The codes must include mechanisms which enable the certification body (approved for this purpose by the competent supervisory authority) to carry out mandatory monitoring of compliance (without prejudice to the powers of competent supervisory authorities). Codes must be approved by the competent supervisory authority which will look at whether it contains sufficient safeguards. Codes which relate to processing activity in more than one Member State will also need further approvals. The European Data Protection Board (the EDPB) will make public all approved codes on a register.

Certification

This is another possible route if it contains binding and enforceable commitments. While certification is encouraged in the GDPR, it appears to be gaining less traction. It involves establishing seals or marks which demonstrate the existence of appropriate safeguards through a certification body. As with the Codes of Conduct, controllers and processors would make binding and enforceable commitments to apply the appropriate safeguards.

Derogations for specific situations

Otherwise, a transfer may take place only on limited grounds such as:

– The data subject has explicitly consented (note that this has been amended from the Directive and data subjects must have been sufficiently informed of the risks of transfer).

– The transfer is necessary for the performance of a contract between the data subject and the controller (or to implement pre-contractual measures taken at the data subject's request).

– The transfer is necessary for the conclusion or performance of a contract, in the interest of the data subject between the controller and another natural or legal person.

– The transfer is necessary for important reasons of public interest, or for the establishment, exercise or defence of legal claims, or to protect the vital interests of a data subject who cannot give consent.

– The transfer is made from a register which, according to Union or Member State law, is intended to provide information to the public and which is open to consultation by anyone with a legitimate interest (only where any conditions for consultation are fulfilled).

Non-repetitive transfers on the basis of legitimate interests

Where none of the above are met, a transfer to a third country or international organisation may only be made if it:

– is not repetitive;

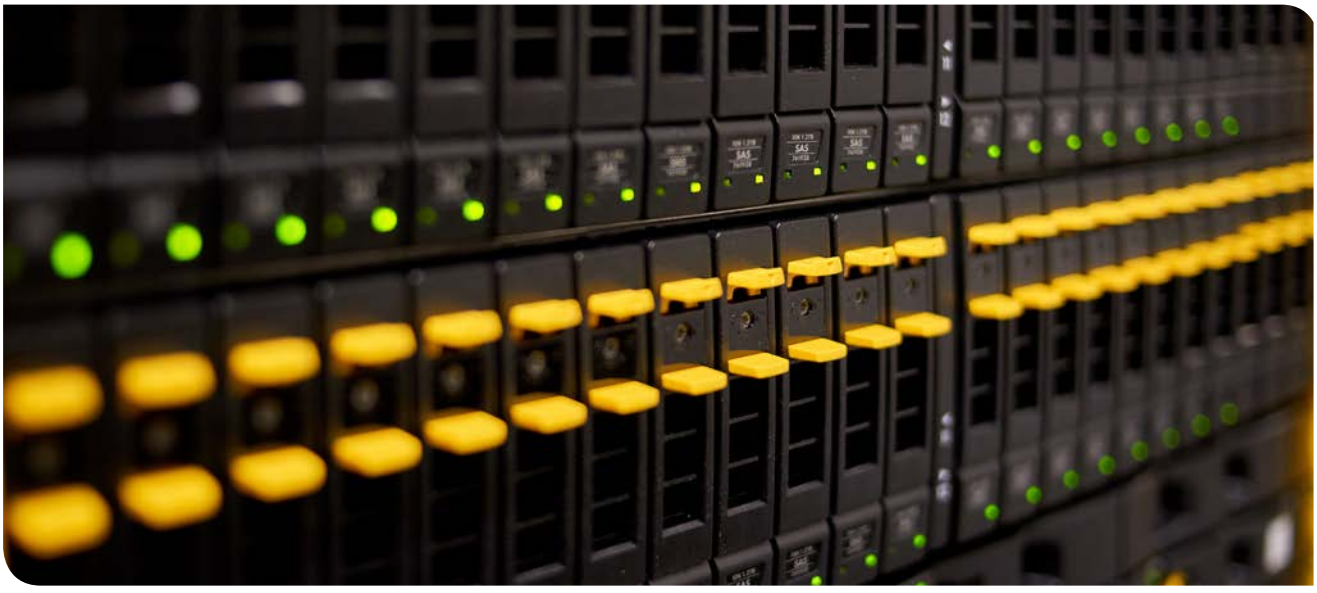
– concerns only a limited number of data subjects;

– is necessary for the purposes of compelling legitimate interests pursued by the controller (and not overridden by the interests or rights and freedoms of the data subject); and

– the controller has assessed all the circumstances and provided suitable safeguards.

A controller who uses this as a basis for transfer must notify the supervisory authority. They must also tell the data subject.

This more restrictive approach in effect replaces self-assessment as a basis for transfer. The self-assessment approach is currently only used as a standalone basis in a few Member States and is arguably a necessary sacrifice in order to achieve uniformity.



Relevant articles & recitals

Article 30 – Records of processing activities – transfers to third countries
Recital 82

Article 40 – Codes of conduct
Recital 98-99

Article 42-43 – Certification
Recital 100

Article 44 – General principles for transfers
Recital 101, 102

Article 45 – Transfers on the basis of an adequacy decision
Recitals 103-107 and 114

Article 46 – Transfers subject to appropriate safeguards
Recitals 108-109

Article 47 – Binding corporate rules
Recital 110

Article 48 – Transfers not authorised by Union law
Recital 115

Article 49 – Derogations for specific situations
Recitals 111-113

Article 50 – International cooperation for the protection of personal data
Recital 116

Impact

– Review your data flows to outside the EEA and consider whether the mechanisms you are using remain appropriate.

– Consider whether BCRs are suitable for intra-group data transfers, or transfers within a group of enterprises engaged in joint economic activity. If you already have BCRs, they will need to be updated. Consider timing for that process and other impacts (eg Brexit).

Remedies, liability and penalties

The GDPR has catapulted data protection compliance into the boardroom by increasing the potential fines significantly.

Under the current regime, for those Member States that can impose monetary penalties, the maximum fines are generally not overly burdensome (eg GBP 500,000 in the UK), although some countries have recently increased the fines (eg EUR 3m in France and EUR 820,000 or up to 10% net annual turnover in the Netherlands).

The GDPR carries fines which can reach the higher of EUR 20m or 4% of annual global turnover for certain breaches

The approach to penalties is tiered depending on the specified nature of the breach. Fines may be in the "up to 2%" (or EUR 10m) or "up to 4%" (or EUR20m) bracket.

When deciding whether to impose an administrative fine and deciding on the amount, the supervisory authority must take into account a number of matters including:

– the nature, gravity and duration of the infringement taking into account the nature, scope or purposes of the processing concerned as well as the number of data subjects affected and the level of damage they have suffered;

– whether the infringement was intentional or negligent;

– action taken in mitigation;

– measures taken to prevent the infringement;

– previous track record;

– the degree of co-operation with the supervisory authority; and

– the manner in which the breach came to the attention of the supervisory authority – did the controller or processor self-report?

As an example of the tiered approach to maximum fine levels, the higher maximum amount applies, among other things, to breach of requirements relating to international transfers and the basic principles for processing, such as conditions for consent. It also applies to the provisions around data subjects' rights.

The GDPR contemplates Member States laying down rules on other penalties applicable to infringements of the GDPR, in particular where they are not subject to administrative fines. This may include, for example, criminal penalties for certain offences.

Supervisory authorities also have a number of new or revised powers under the GDPR, which include the ability to carry out audits, to order remediation within a specific time frame, to order erasure of data and to suspend data transfers to a recipient in a third country.

This is an area where it will be particularly important to review implementing legislation, which will elaborate considerably in many areas on the text of the GDPR.

Data subjects will under GDPR have a cause of action, for the first time, against data processors (to seek compensation). The claim may relate to breach of the GDPR or failure to follow the controller's instructions.

In general, data subjects will be entitled to seek compensation from controllers and processors for material and non-material damage (including non-financial loss). Group actions are encouraged by provisions allowing for representative bodies to bring claims.

The GDPR explicitly provides for the possibility of joint liability for controllers and processors where they are jointly responsible for damage. Claims may be brought either in the courts of the Member State of the controller or processor's establishment or where data subjects naturally resides.

Relevant articles & recitals

Article 58 – Powers

Article 82 – Right to compensation and liability

Article 83 – General conditions for imposing administrative fines

Recitals 147-148 and 150-152

Article 84 – Penalties

Recital 149, 152

Impact

– When developing policies, bear in mind the factors that supervisory authorities will take into account when setting fines in particular, the organisation's approach to notifying breaches and co-operation with relevant supervisory authority(ies).

– Develop a policy/procedure for responding to an audit or request for information.

– Check the position on liability in relevant contracts with third parties (such as agreements with suppliers or customers).

– Consider implementing legislation for details of procedures applicable in relevant Member States.

Supervisory authorities

Data controllers and data processors operating across more than one Member State will need to identify their main establishment.

One of the key questions companies are grappling with is the identity of their Lead Supervisory Authority under the GDPR. This is important because the lead supervisory authority will play a key role in regulating compliance by that company with the GDPR. The lead authority will have primary responsibility for dealing with cross border data processing activity, including handling and investigating complaints lodged by data subjects and imposing any resulting sanctions.

Companies operating in one Member State

Where a company has a single establishment in the EU and its activities do not substantially affect data subjects in other Member States, things are more straightforward. These companies will simply have one supervisory authority in the Member State of their establishment.

Companies that carry out cross-border processing

"Cross-border processing" is defined by the GDPR as either processing in the context of activities (i) of its establishments in more than one Member State or (ii) of a single establishment in the EU but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Those who carry out cross border processing should seek to identify their lead supervisory authority by determining the location of their "main establishment".

The "main establishment" test

The "main establishment" for a data controller is the place of its central administration in the EU, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment (which has the power to implement them), which would then be considered the "main establishment".

For a data processor, it is the place of its central administration in the EU, or if it has none, the establishment in the EU "where the main processing activities in the context of an establishment of the processor take place" to the extent it is subject to the GDPR.

Note that where both a controller and a processor are involved, the controller's lead authority will be competent as lead.

While the Article 29 Working Party are keen to avoid forum shopping, their guidance suggests that there is some room for manoeuvre if a business does not have an obvious main establishment. However, they have made it clear that if a company claims to have a lead authority in a Member State but does not meet the tests set out above, the relevant supervisory authorities (and ultimately the EDPB) could ask them to evidence their decision and may challenge it, deciding on the "lead" by looking at the facts.

Working with the Supervisory Authority

Once the main (or single) establishment has been identified, the controller or processor must communicate to their lead authority the details of their data protection officer (where they have one). They must also cooperate, on request, with the supervisory authority in the performance of their tasks. Many consider that it is best practice to start a dialogue with the lead authority as early as possible, particularly where, for example, the organisation has BCRs in place.

There are cases where a company may have more than one lead supervisory authority. The company may make decisions for different cross border processing in separate decision-making centres. It may be difficult to determine where main decisions are taken.

Those companies that do not have an "establishment" in any Member State will not benefit from having a lead supervisory authority and will have to deal individually with the regulator in each jurisdiction in which they are caught by the GDPR.

The GDPR creates a cooperation and consistency regime between supervisory authorities called the "One Stop Shop"

Where a company has a lead supervisory authority, the One Stop Shop regime applies. This is a set of complex cooperation and coordination procedures for the supervisory authorities to follow to ensure that all relevant authorities have a say.

Supervisory authorities in other Member States may be involved as "concerned authorities" where, for example, the controller has an establishment in their jurisdiction, or data subjects are substantially affected in that authority's Member State. There is an exception for local cases and urgent cases which can be handled appropriately.

The lead authority must cooperate with the concerned authorities in an endeavour to reach consensus, including submitting draft decisions to them without undue delay and taking account of their views. If the lead authority does not agree with any relevant and reasoned objections raised, they must submit to the consistency procedure which is supervised by the European Data Protection Board.

The process of going through the EDPB and its rounds of voting is complex. The EDPB has a month (which can be extended by a further month) to agree on a binding decision by a two third majority vote. However, if they cannot agree within the two months, they have a further two weeks to agree by simple majority. This could become a somewhat political process and we may see block voting by some Member States' supervisory authorities in alliance. This could make the mechanism a very unwieldy tool for ensuring consistency in decision-making and there is a concern that cases may get stuck in the process, despite the timeframes stipulated, given the limited resources of the EDPB. This will depend on the number of cases referred.

Supervisory authorities have to exchange information, and the lead authority may request mutual assistance, for example in order to apply the GDPR in a consistent manner. It may also conduct joint operations, such as joint investigations.

It is not yet clear how well this system will work in practice. Even where a lead supervisory authority is agreed upon, the system relies heavily on that lead authority agreeing with any concerned authorities. Data protection authorities are not used to having to work together so closely in this way and have often taken very different approaches to dealing with cases.

Relevant articles & recitals

Article 4 – Definition of "main establishment", "cross border processing", "relevant and reasoned objections" and "supervisory authority concerned"
Recital 36

Article 31 – Co-operation with the supervisory authority
Recital 82

Article 51 – Supervisory authority
Recitals 116-117

Article 55 – Competence (of the supervisory authority)
Recitals 20 and 122

Article 56 – Competence of the lead supervisory authority
Recitals 36, 124-125 and 128

Article 57 – Tasks of the supervisory authorities
Recitals 120-123 and 132

Article 58 – Powers of the supervisory authorities
Recitals 129, 131 and 150

Article 60 – Cooperation between supervisory authorities
Recitals 116, 125-128, 130-131 and 133-134

Article 61 – Mutual assistance
Recital 123, 133

Article 62 – Joint operations
Recital 134

Article 63 – Consistency mechanism
Recitals 119, 123, 128-129, 135-136, 139 and 141

Article 66 – Urgency procedure
Recitals 137-138

Impact

– If you carry out activities in more than one Member State, you should assess where your main establishment is and determine if you have a lead supervisory authority.

– Where the case is not clear cut, it would be worth seeking advice about nominating a main establishment.

– If your main establishment is currently in the UK, this is unlikely to be an option after Brexit for cross-border data processing.

– Once you have identified your lead supervisory authority, engage with it as you prepare for the GDPR, for example by looking at any guidance or support it is offering.

What next?

Getting GDPR-ready requires a significant effort and the input and assistance of many business functions.

You will need to review systematically your existing data processing activities, and how you are going to collect and use data in the future, to ensure you are compliant. It is inevitable for many businesses that systems will need to be replaced or upgraded, and practices altered, in order to meet the challenges posed by the GDPR.

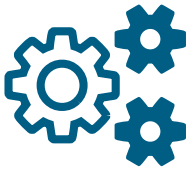
Phase 1: Initial assessment

Assess at a high level the GDPR requirements against the activities of the organisation. This will help to define the project scope for subsequent phases, as well as define the baseline requirements of a GDPR compliant privacy programme.

Phase 2: Data gathering and gap analysis

Analyse:
– current processing activities (including data flows)
– current compliance steps

Carry out a gap analysis against GDPR readiness criteria. This should not be an exercise in archaeology, but rather of identifying specific areas where enhancements to existing activities may be required.



Phase 3: Remediation plan

Plan specific actions which should be undertaken to achieve a GDPR-compliant privacy programme. This should include steps planning and prioritisation.

Phase 4: Implementation

Implement the remediation plan. Most companies will commence the implementation phase in parallel with Phases 1 to 3 to ensure prompt attention is given to high risk items and also to take advantage of quick wins.

We recommend assessment of GDPR readiness against the following pillars:

Strategic outlook

Examine the level of awareness about data protection risks and principles throughout the business. Consider how well data privacy considerations are built into senior decision making processes and how well data is exploited and managed within the business.

Privacy by design

Examine how well you currently implement the principles of privacy by design and by default into your new products, services, systems and business processes, as well as the level of awareness of and training in respect of these practices within the business.

Governance

You should look at the governance of data protection within your organisation, with a view to the potential role of data protection officers under the GDPR.

Security

Review at a legal, non-technical level, the steps presently taken by your organisation to ensure data security. This may include use of anonymisation, encryption and other techniques. You should also focus on your existing data breach notification processes, as well as your approach to contracting with third parties that process your data (including due diligence, standard terms and audit mechanisms).

Accountability and policy

Consider how well your organisation is able to demonstrate compliance with data protection law, including through appropriate documentation, by articulating your overall compliance programme, through policies, by your data inventories and data flow mapping, and by your conduct of data protection impact assessments and other risk management tools. Examine the extent to which you have, and have an understanding of, the lawful basis for processing personal data under the GDPR, including special categories of data, the processes to ensure data quality, to limit access to data, to ensure functional separation of data to limit use to lawful purposes, to data minimisation and data retention, and in relation to profiling and automated decision-making.

Data subject rights

Bearing in mind the strengthened rights that individuals enjoy under the GDPR relating to the processing of their personal data (such as the right to access personal data, the right to be forgotten and the right to data portability), you should examine whether you have adequate existing processes in place.

Transparency

Examine the extent to which information you provide to individuals needs to be supplemented or revised to meet GDPR requirements, including whether you currently provide fair processing information in all circumstances where it is required.

Outsourcing, data sharing and data transfers

Check the extent to which your standard agreements with suppliers contain the minimum provisions required under the GDPR. If you engage a third party to carry out processing operations on your behalf, remember that you are required to enter into a data processing agreement that complies with the requirements set out in the GDPR. You should also review your existing mechanisms and processes in relation to cross-border data transfers, both within the group and to third parties.

Monitoring and verification

Review your ability to respond to audit enquiries under the GDPR, as well as to engage proactively with the supervisory authority where required (eg for prior consultation).

Contacts

Jane Finlayson-Brown
Partner – London
Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

Nigel Parker
Partner – London
Tel +44 20 3088 3136
nigel.parker@allenovery.com

David Smith
Peerpoint Consultant – London
Tel +44 20 3088 6842
david.a.smith@allenovery.com

Charlotte Mullarkey
Counsel – London
Tel +44 20 3088 2404
charlotte.mullarkey@allenovery.com

Sarah Henchoz
Partner – London
Tel +44 20 3088 4810
sarah.henchoz@allenovery.com

Mark Mansell
Partner – London
Tel +44 20 3088 3663
mark.mansell@allenovery.com

Anita Anand
Senior Associate – London
Rulefinder Cross-Border Data Transfer
Tel +44 20 3088 2831
anita.anand@allenovery.com

Livio Bossotto
Counsel – Milan
Tel +39 02 2904 9678
livio.bossotto@allenovery.com

Romaric Lazerges
Partner – Paris
Tel +33 14 006 5344
romaric.lazerges@allenovery.com

Laurie-Anne Ancenys
Counsel – Paris
Tel +33 140 065 342
laurie-anne.ancenys@allenovery.com

Wanne Pemmelaar
Senior Associate – Amsterdam
Tel +31 20 674 1443
wanne.pemmelaar@allenovery.com

Emre Yildirim
Associate – Amsterdam
Tel +31 20 674 1339
emre.yildirim@allenovery.com

Tobias Neufeld
Partner – Düsseldorf
Tel +49 211 2806 7120
tobias.neufeld@allenovery.com

Antonio Martinez
Partner – Madrid
Tel +34 91 782 99 52
antonio.martinez@allenovery.com

Filip Van Elsen
Partner – Antwerp
Tel +32 3 287 73 27
filip.vanelsen@allenovery.com

Peter Van Dyck
Partner – Brussels
Tel +32 2 780 25 12
peter.vandyck@allenovery.com

Catherine Di Lorenzo

Counsel – Luxembourg
Tel +352 44 44 5 5129
catherine.dilorenzo@allenovery.com

Charles-Henri Laevens

Juriste – Luxembourg
Tel +352 44 44 5 5282
charles-henri.laevens@allenovery.com

Zuzana Hecko

Senior Associate – Bratislava
Tel +421 2 5920 2438
zuzana.hecko@allenovery.com

Roxana Ionescu

Senior Associate – Bucharest
Tel +40 31 4057777
roxana.ionescu@rtprallenovery.com

Balazs Sahin-Toth

Counsel – Budapest
Tel +36 1 429 6003
balazs.sahin-toth@allenovery.com

Krystyna Szczepanowska-Kozłowska

Partner – Warsaw
Tel +48 22 820 6176
krystyna.szczepanowska-kozlowska@allenovery.com

Justyna Ostrowska

Senior Associate – Warsaw
Tel +48 22 820 6172
justyna.ostrowska@allenovery.com

Prokop Verner

Partner – Prague
Tel +420 222 107 140
prokop.verner@allenovery.com

Ondrej Kramolis

Senior Associate – Prague
Tel +420 222 107 196
ondrej.kramolis@allenovery.com

GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,400 people, including some 554 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

Abu Dhabi
Amsterdam
Antwerp
Bangkok
Barcelona
Beijing
Belfast
Bratislava
Brussels
Bucharest (associated office)
Budapest
Casablanca
Doha
Dubai
Düsseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Istanbul
Jakarta (associated office)
Johannesburg
London
Luxembourg
Madrid
Milan
Moscow
Munich
New York
Paris
Perth
Prague
Riyadh (cooperation office)
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.
Yangon

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term **partner** is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.