

THE EU GENERAL DATA PROTECTION REGULATION

A guide for in-house lawyers

January 2017

HUNTON &
WILLIAMS

Index

Introduction to the Regulation	-	3
Progress of the Regulation	-	4
Using this Guide	-	5
Conceptual Overview	-	6
Definitions	-	8
Jurisdiction and Territorial Scope	-	10
Enforcement, Sanctions and Penalties	-	12
Supervisory Authorities	-	14
Accountability	-	16
Information Notices	-	18
Data Protection by Design and by Default / DPIAs	-	20
Profiling	-	22
Data Breach Reporting	-	24
Obligations of Processors	-	26
Processing Conditions	-	28
Anonymisation and Pseudonymisation	-	30
Cross-Border Data Transfers	-	32
Binding Corporate Rules	-	34
Seals, Certifications and Codes of Conduct	-	36
Rights of Data Subjects	-	38
Areas Remaining Unharmonised	-	40
Glossary	-	42
Our Team	-	43

© 2017 Hunton & Williams. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.

Introduction to the Regulation

Background

- **Existing law:** Current EU data protection law is based on Directive 95/46/EC (the “**Directive**”), which was introduced in 1995. Since that time, there have been significant advances in information technology and fundamental changes to the ways in which individuals and organisations communicate and share information. In addition, the various EU Member States have taken divergent approaches to implementing the Directive, creating compliance difficulties for many businesses.
- **Changes:** The EU’s legislative bodies have prepared two updated legal instruments to replace the Directive. A specific directive will cover personal data held for the purposes of criminal justice and policing and an updated and harmonised regulation (the “**Regulation**”) will cover all other processing. The Regulation will significantly change EU data protection law in several areas. As described on page 4, the Regulation will be adopted in Spring 2016. Organisations will have a 2 year transitional period to implement changes and comply with the new law. The Regulation shall apply from Spring 2018.

Background to the Regulation











As with any EU legislation, there has been detailed negotiation before the final version has been agreed.

- **The Commission Text** – The Commission published the first draft of the Regulation on 25 January 2012.
- **The Parliament Text** – The Parliament adopted a series of proposed amendments to the Commission Text on 12 March 2014.
- **The Council Text** – The Council released its final text on 16 December 2015.

PLEASE NOTE: This Guide should be used as general guidance only and should not be relied upon as legal advice. You are welcome to re-use the content of this Guide, provided you credit Hunton & Williams using the copyright notice set out on page 2, and any use is limited to within your organisation. Please also note that the Directive and (to a lesser extent) the Regulation are subject to national interpretation. This Guide is not designed to provide analysis of national requirements. For advice on these issues, and other more detailed questions, please contact:

EUregulation@hunton.com

Progress of the Regulation

	 European Commission	 European Parliament	 Council of the European Union	 Other Interested Parties
Denmark Jan - Jun 2012	<ul style="list-style-type: none"> January 2012  Commission Text published by Vice-President Viviane Reding. 	<ul style="list-style-type: none"> May 2012 – The European Parliament held an initial stakeholder meeting. 		<ul style="list-style-type: none"> February 2012 – The UK DPA published initial comments on the proposed Regulation.
Cyprus Jul - Dec 2012		<ul style="list-style-type: none"> July 2012  First Parliament working document (“LIBE Text”) published. 		
Ireland Jan - Jun 2013		<ul style="list-style-type: none"> January 2013  Text released by Jan Philipp Albrecht, the Parliamentary Rapporteur. 	<ul style="list-style-type: none"> May 2013  Compromise Text released by the Council. 	<ul style="list-style-type: none"> January 2013 – The French DPA released an Opinion on the proposed Regulation.
Lithuania Jul - Dec 2013		<ul style="list-style-type: none"> Autumn 2013 – Informal negotiations between the Parliament and the Council on the basis of the Compromise Text. 		
Greece Jan - Jun 2014		<ul style="list-style-type: none"> March 2014  Parliament Text adopted following vote in the Parliament. 	<ul style="list-style-type: none"> June 2014 – EU Ministers agreed rules on the territorial application of the Regulation (see pages 10-11). 	<ul style="list-style-type: none"> May 2014 – Decision of the CJEU in <i>Costeja v. Google</i>, concerning the “<i>right to be forgotten</i>” (see page 38).
Italy Jul - Dec 2014			<ul style="list-style-type: none"> October 2014 – EU Ministers partially agreed the “<i>risk-based approach</i>” (see page 20). 	
Latvia Jan - Jun 2015			<ul style="list-style-type: none">  EU Ministers work towards a final Council Text. 	
Luxembourg Jul - Dec 2015	<ul style="list-style-type: none"> A “trilogue”, involving the Council, the Parliament and the Commission, began with the aim of finalising the text of the Regulation. This was a complex process that resulted in the publication of the final Regulation text for approval on 16 December 2015. 			<ul style="list-style-type: none"> October 2015 – Decision of CJEU in <i>Schrems</i> invalidated Safe Harbour.
Netherlands Jan - Jun 2016	<ul style="list-style-type: none"> Spring 2016 The Final Text of the Regulation was jointly agreed by the Commission, the Parliament and the Council in Spring 2016. The Regulation shall apply from Spring 2018. 			<ul style="list-style-type: none"> January 2016 – US and EU agree on new Privacy Shield.

Using this Guide

The purpose of this Guide is to provide in-house lawyers with the tools to:

- understand the key impacts of the Regulation on businesses; and
- explain those impacts to business decision-makers.

This Guide provides an overview of the topics in the Directive and the Regulation that are most likely to affect businesses. There are two pages for each topic:



The page on the right uses the following symbols:



Some things stay the same – Although the language of the Regulation often differs from the Directive, there are many issues for which the outcome is essentially the same. For each such issue, the text is shown in two grey boxes (the Directive on the left; the Regulation on the right) with an “approximately equals” sign between them, to indicate that there are no significant changes.



Some things materially change – There are a number of areas in which the Regulation introduces changes that are likely to impact businesses. For these issues, the concepts are shown in blue, with an arrow between them, indicating the change.



Some changes are broadly **positive for most businesses** (e.g., because they reduce the relevant compliance burden or provide greater certainty).



Some changes **make little practical difference** for most businesses (e.g., because the new requirements create no new costs or burdens).



Some changes are broadly **negative for most businesses** (e.g., because of increased compliance obligations or more severe penalties for non-compliance).



Cross-referencing – To enable easy cross-referencing to the original text, Articles from the Directive and the Regulation are identified with indented arrows where appropriate.

Defined terms and abbreviations used in this Guide are explained in the **Glossary** on page 42.

Conceptual Overview



Why is this issue important for businesses? Understanding the background to the EU's data protection laws, as well as the changes that the Regulation will bring, is vital to any business assessing its data protection compliance obligations.



Affected sectors: All business sectors are likely to be affected by the proposed changes to EU data protection law that the Regulation will introduce.

- **Before 1995:** Until the mid-1990s, businesses operating in the EU faced different compliance obligations across the EU, depending upon national legal requirements.
- **The Directive:** Introduced in 1995, the Directive created a broadly consistent set of data protection laws for the EU. The Directive (like any EU Directive) needed to be transposed into the national laws of Member States. Consequently, although the general principles of data protection law are similar across the EU, there remain differences between the laws of each Member State, and so businesses continue to face conflicting requirements.
- **New technologies:** With the rise of the internet, technology evolved rapidly and the ways in which personal data could be used by businesses expanded. The explosive growth of cloud computing, social networking and big data analytics (among other things) made it increasingly clear that a new approach to data protection was required.
- **The Regulation:** The Regulation is designed to further harmonise national data protection laws across the EU while, at the same time, addressing new technological developments. The Regulation will be directly applicable across the EU, without the need for national implementation. Businesses are likely to face fewer national variations in their data protection compliance obligations. However, as noted on page 7, there remain areas in which there will continue to be differences from one Member State to another.
- **Some concepts stay the same:** The law still applies to all personal data, and responsibility for compliance continues to be allocated to parties in the roles of 'controller' and 'processor'.
- **Some concepts change, and are likely to be good for businesses:** For example, the increased harmonisation of data protection laws across the EU should result in fewer conflicting obligations and should make it easier to do business across the EU, relying on a single set of principles. Similarly, national registration of processing with DPAs is abolished in favour of an internal register.
- **Some concepts change, and are likely to present challenges for businesses:** In particular, new penalties (including fines of up to 4% of annual worldwide turnover) are such a significant departure from the existing regime that they constitute a conceptual change. Data protection will be as significant as antitrust or anti-corruption in terms of compliance risk. Under the Regulation, data protection will no longer be an area in which businesses can afford to take casual risks.
- **Going forward:** The Regulation is likely to require organisation-wide changes for many businesses. In-house lawyers should start to consider the impact of those changes and plan ahead. Failure to do so could mean that businesses are left with new requirements to implement, without having set aside appropriate resources.

The Directive

The Regulation

Purpose: The purpose of the Directive is to provide a set of rules to govern the processing of personal data.



Purpose: The purpose of the Regulation is to provide a new set of rules to govern the processing of personal data, replacing the Directive.

Scope: The Directive covers data protection law on an EU-wide basis, and applies to both public and private sectors.



Scope: The Regulation covers data protection law on an EU-wide basis, but also has extra-territorial effect (see page 10). (A separate EU Directive, operating in parallel with the Regulation, will cover the processing of personal data in connection with the prevention, detection, investigation or prosecution of criminal offences and related judicial activities.) The Regulation applies to both public and private sectors.

Implementation: The Directive needed to be implemented at a national level, requiring transposition into national law by the national legislature of each Member State.



Implementation: The Regulation is directly applicable in all Member States. This means that the Regulation applies automatically in each Member State and (subject to the specific exceptions noted on page 40) it does not require any national implementation by Member States.

Application: The Directive is an 'omnibus' privacy law – it applies across all business types and all sectors.



Application: The Regulation is an 'omnibus' privacy law – it applies across all business types and all sectors.

Harmonisation: Under the Directive, data protection law varies from one Member State to another, depending on national approaches to implementation and enforcement. These differences can be significant (e.g., in some Member States there is no obligation to register as a controller; in others it is a criminal offence to fail to do so).



Harmonisation: Under the Regulation there is much greater harmonisation between the national data protection laws of Member States, because there is no need for national implementation. However, differences remain in a few areas (e.g., in relation to employment law and national security – see page 41).

Enforcement: Enforcement of the Directive (as implemented into national law) is carried out by national DPAs.



Enforcement: Enforcement of the Regulation is carried out by national SAs. However, the Consistency Mechanism is intended to ensure that national SAs apply the Regulation consistently across the EU. In addition, the EDPB will play a significant part in enforcement decisions through the Consistency Mechanism (see pages 14-15).

Fines: Penalties are determined by national law and the maximum penalties are generally comparatively low (e.g., in the UK, the largest single fine issued to date is £250,000, and in other Member States fines have not exceeded the low millions of Euros).



Fines: Penalties are specified in the Regulation. The maximum penalty is **€20 million or 4% of annual worldwide turnover**, whichever is greater.

Definitions



Why is this issue important for businesses? Definitions form the building blocks of both the Directive and the Regulation. Understanding the nature and extent of the changes to these definitions is critical to understanding the Regulation.



Affected sectors: All business sectors will be affected by these new definitions.

- **Continuity of many core definitions:** Many of the core definitions from the Directive (e.g., 'controller', 'processor' and 'processing') are essentially unchanged under the Regulation.
- **Practical benefits of continuity:** The continuity of these definitions means that it is possible to build upon existing compliance structures and commercial arrangements, rather than starting again. For example:
 - *Employee training* – If a business has already trained its employees to identify 'personal data', that training remains useful. Any data that were personal data under the Directive continue to be personal data under the Regulation.
- **Consent becomes harder to obtain:** In particular, the definition of 'consent' makes valid consent significantly more difficult to obtain (see page 28). Businesses that rely on consent will need to carefully review their existing practices and ensure that any consent they obtain is specific, and indicates unambiguous agreement from the data subject (e.g., ticking a blank box). Controllers must be able to demonstrate that consent was validly obtained.
- **Personal data of children:** The Regulation includes a requirement to obtain parental consent to the processing of personal data relating to a child under 16 years of age, or at a lower age depending on Member State law, which cannot be below 13. It is important for businesses to consider how best to achieve this (particularly in an online context where identities can be difficult to verify).
- **Genetic data:** Genetic data are not explicitly mentioned in the Directive. Under the Regulation, genetic data used to uniquely identify individuals are explicitly defined as sensitive personal data. Businesses that use such data will need to consider whether changes to their business practices are required.

PLEASE NOTE: The comparison on page 9 (opposite) illustrates significant changes. However, in some cases, comparatively minor definition changes may still affect businesses. For example, the new definition of 'personal data' explicitly includes items such as online identifiers and location data. These items are often treated as personal data under the Directive, but some businesses have sought to argue that this is not the case. Under the Regulation, they will clearly be personal data, and affected business practices will need to be amended accordingly.

The Directive

The Regulation

Art.2

'**consent**': any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

'**controller**': the person or body that, alone or jointly with others, determines the purposes and means of the processing of personal data.

'**personal data**': any information relating to an identified or identifiable natural person (a '**data subject**'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

'**genetic data**': there is no definition of 'genetic data' in the Directive.

Art.8(1)

'**sensitive personal data**': personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life. Several Member States have added actual or alleged criminal offences to this list.

Art.4

'**consent**': any freely given, specific, informed and *unambiguous* indication of his or her wishes by which the data subject, *either by a statement or by a clear affirmative action*, signifies agreement to personal data relating to him or her being processed.

'**controller**': the person or body that, alone or jointly with others, determines the purposes, and means of the processing of personal data.

'**personal data**': any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'**genetic data**': all personal data relating to the genetic characteristics of an individual that have been inherited or acquired which give unique information about the physiology or the health of the individual resulting in particular from an analysis of a biological sample from the individual in question.

Art.9

'**special category personal data**': personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, *genetic data or biometric data* or data concerning health or sex life, or *sexual orientation*.

Jurisdiction and Territorial Scope



Why is this issue important for businesses? Understanding whether the Regulation will apply to a business or not (particularly if that business is established outside the EU) is fundamental to identifying that business's compliance obligations.



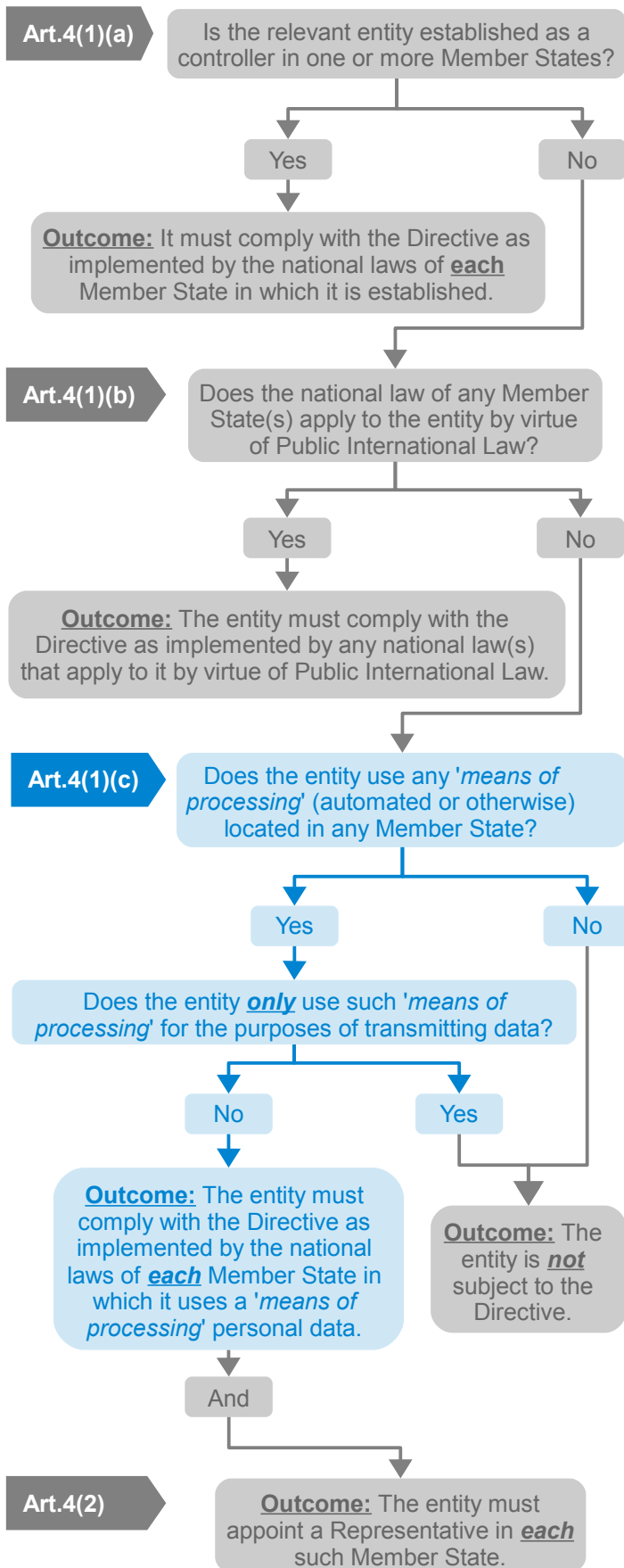
Affected sectors: This issue is of particular relevance to businesses that are based outside the EU, but conduct business in the EU.

- **For businesses established in the EU:** Currently if a data controller is established in any Member State, then it is subject to the Directive as implemented by national law in that Member State.

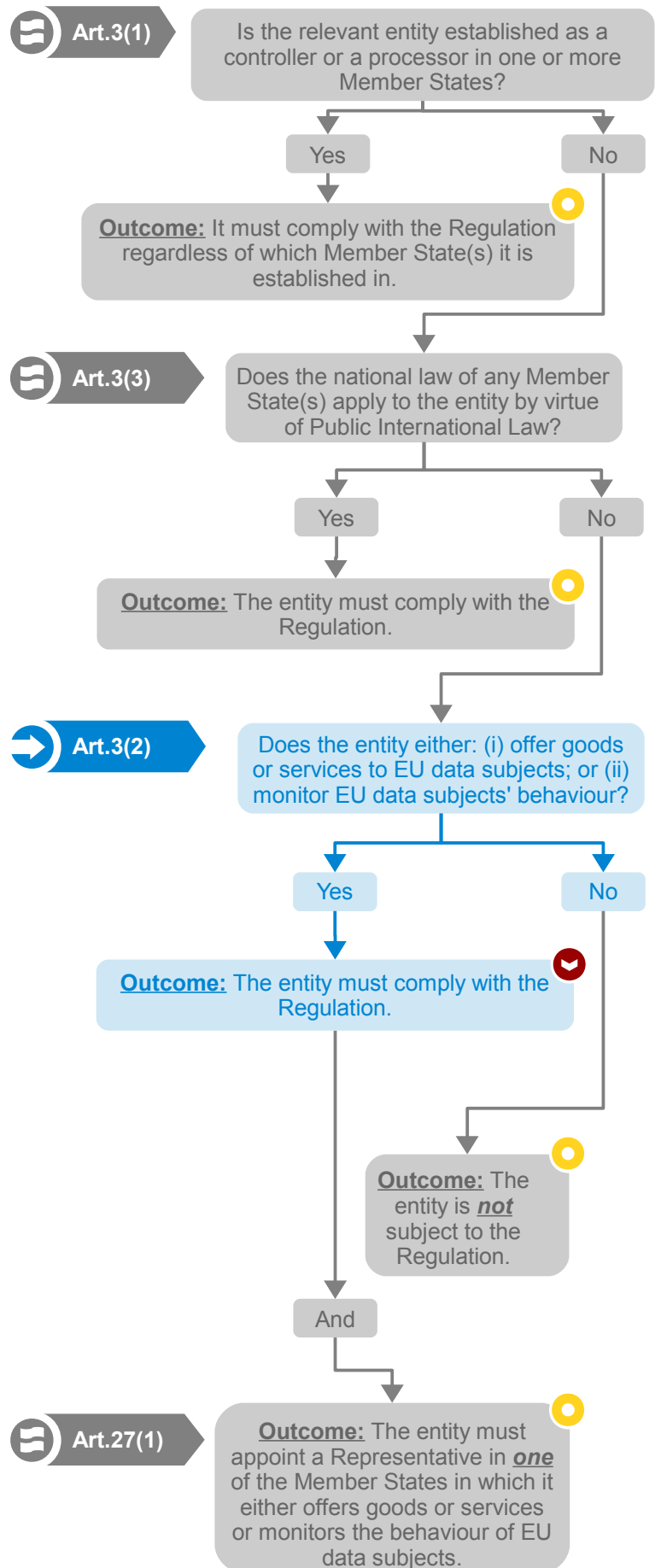
Established data controllers and processors will be subject to the Regulation as it applies in that Member State; however, many of the provisions will apply directly and will not require implementation by national legislation.
- **For businesses based outside the EU, the requirements change:** The test for determining whether EU data protection law applies to entities established in non-EU jurisdictions will change significantly:
 - **Under the Directive:** EU data protection law only applies to an entity established outside the EU that uses equipment situated in the EU to process personal data, unless that equipment is only used for the purposes of simply transmitting data.
 - **Under the Regulation:** The test in the Directive is replaced by a new test. If a data controller or a data processor is established outside the EU, and it either:
 - (i) offers goods or services to data subjects in the EU; or
 - monitors the behaviour of data subjects in the EU, that entity will be subject to the Regulation.
- **For example:** A business established in the US that markets its products directly to the EU, but has no physical presence in the EU, is not subject to the requirements of the Directive, but will be subject to the requirements of the Regulation.
- **The obligation to appoint a Representative:** Under the Regulation an entity based outside the EU will have an obligation to appoint a representative in a single Member State. The Representative functions as the entity's point of contact for SAs (although SAs are not obliged to contact the Representative and may choose to deal directly with the relevant controller or processor).
- **Going forward:** Businesses established outside the EU should consider whether any of their entities are subject to the Regulation. If so, such a business should review the compliance obligations of its affected entities under the Regulation, as set out in this Guide.

PLEASE NOTE: The flow-chart on page 11 is designed to assist with the analysis of these issues. This flowchart is designed on a per-entity basis – it does not work for corporate groups collectively. Under both the Directive and the Regulation, it is possible that some entities within a corporate group will have compliance obligations under EU data protection law, while other entities will not.

The Directive



The Regulation



Enforcement, Sanctions and Penalties



Why is this issue important for businesses? The likelihood of enforcement and the magnitude of any applicable sanctions (orders, fines, actions by individuals) and penalties (criminal punishment) influence a business's approach to compliance. The Regulation makes significant changes in this area.



Affected sectors: All business sectors will be subject to the new enforcement powers, sanctions and penalties that the Regulation imposes.

- **Enforcement powers:** Under the Directive, the powers of national DPAs are not specified beyond requiring broad investigative and enforcement powers. Instead, the Directive leaves the detail of DPA enforcement powers to individual Member States. The Regulation will grant SAs specific investigative and enforcement powers.
- **Sanctions and penalties:** Under the Directive, the penalties and sanctions for breaches of national data protection law are not harmonised, and vary considerably across different Member States. The Regulation sets out the range of applicable administrative sanctions for breaches of certain aspects of the Regulation. Individual SAs will retain discretion to determine the particular sanction to be applied in a given case, but the maximum sanctions will be prescribed by the Regulation. Criminal penalties are decided by Member States but will be mandatory.
- **Enforcement actions:** Under the Directive, the circumstances in which DPAs may take enforcement action are not prescribed. For example, in Spain, the DPA is required by law to investigate all complaints received, but this is not the case in other Member States. Under the Regulation, data subjects will be entitled to obtain a court remedy requiring the SA to deal with a complaint.
- **Harmonisation:** The Regulation will harmonise enforcement powers across the EU (including through the Consistency Mechanism) – see page 14.
- **Significantly increased sanctions and penalties:** The Regulation will prescribe the administrative sanctions applicable to breaches of the Regulation, and will harmonise the approach to enforcement across the EU. This will result in a substantial increase in the maximum possible fine. For example, the current maximum fine in the UK is £500,000 and the largest single fine issued to date is £250,000. Under the Regulation, the maximum fine will become the greater of **€20 million or 4% of annual worldwide turnover**.
- **Judicial remedies:** The Regulation will grant data subjects the right to obtain a judicial remedy against an SA, requiring the SA to deal with the data subject's complaint. Data subjects also have a right of judicial remedy against controllers or processors as well as a right to obtain compensation for breaches of the Regulation.
- **Going forward:** Businesses that have not previously regarded non-compliance with EU data protection law as a serious risk will need to re-evaluate their positions in light of the substantial new fines and increased SA enforcement powers.

The Directive

Art.22

Remedies: Under the Directive, Member States must provide every data subject with the right to a judicial remedy for breach of any of his or her data protection rights. In practice, the rights of data subjects differ across Member States.



Art.23

Compensation: Under the Directive, Member States must provide a right for data subjects to recover compensation from any controller who processes personal data unlawfully.



Art.24

Sanctions: Under the Directive, Member States are required to impose sanctions on controllers for breach of national data protection law. The Directive does not specify the sanctions to be imposed.



Art.28

DPA enforcement powers: DPAs have the following minimum powers, under national law:

- investigative powers;
- powers of intervention (e.g., to order the blocking, erasure or destruction of data); and
- the power to commence legal proceedings.



The Regulation

Art.78 & 79

Right to a remedy against an SA: Under the Regulation, all data subjects will have the right to go to court to make the SA deal with a complaint by the data subject. In addition, the Regulation will provide businesses and data subjects with a right to appeal against a decision of the SA.

Right to a remedy against a controller or processor: Data subjects will have the right to take court action in respect of any processing of their personal data that infringes the Regulation.

Art.82

Compensation: All data subjects will have the right to obtain compensation from the relevant controller *or processor* for damage suffered as a result of processing carried out in breach of the Regulation.

Art.83

Sanctions: The fines applicable for breaches of the Regulation include:

- for a failure to obtain parental consent where personal data are collected about a child in the process of providing an information society service, **a fine of up to €10m or 2% of the controller's annual worldwide turnover of the preceding year**; and
- for a failure to provide adequate information to data subjects or to allow subject access, or to comply with the right to erasure (amongst others), **a fine of up to €20m or 4% of the controller's annual worldwide turnover of the preceding year**.

Art.58

SA enforcement powers: SAs will be given wide-ranging powers to enforce compliance with the Regulation (e.g., the power to compel a controller or processor to provide any information relevant to the performance of the SA's duties, and the power to impose a ban on processing).

Supervisory Authorities



Why is this issue important for businesses? The Directive is enforced by national DPAs, which have a significant degree of autonomy. Under the Regulation, SAs will be obliged to enforce the law consistently across the EU.



Affected sectors: Businesses in all sectors will be subject to investigation of their processing activities, and enforcement of the Regulation, by SAs.

- **The Directive:** Under the Directive, each Member State has created a national DPA, tasked with enforcing the Directive, as implemented under the national law of that Member State. The DPA may investigate breaches of national data protection law and bring enforcement action in the event of a breach of that law. The DPA is generally the main forum to which data subjects bring complaints.
- **The Regulation:** Under the Regulation, each Member State must create one or more SAs. SAs will fulfil broadly the same role that DPAs fulfil under the Directive, and most Member States will transition their existing DPA into the SA role when the Regulation comes into force. As with the position under the Directive, each SA will investigate breaches of the Regulation and bring enforcement action in the event of a breach. The SA will provide the main forum to which data subjects bring complaints.
- **The 'One Stop Shop':** Under the Regulation, where a business has multiple establishments in the EU or just one establishment but carries out processing that affects individuals in other Member States, it will have a single SA as its 'lead authority', based on the location of its sole or 'main establishment' (i.e., the place where the main processing activities take place). The lead authority will act as a 'One Stop Shop' to supervise all the processing activities of that business that have an impact throughout the EU.
- **The Consistency Mechanism:** In order to ensure that the Regulation is enforced uniformly across the EU, the Regulation will require the lead authority to consult with the other concerned authorities in cases in which enforcement action by a lead authority affects processing activities in more than one Member State. A wide range of issues will fall under the Consistency Mechanism (e.g., multi-jurisdictional enforcement issues, BCRs, etc.).
- **The EDPB:** Under the Regulation, the EDPB will effectively replace the WP29. Its tasks will include advising the EU institutions on data protection issues, overseeing the application of the Consistency Mechanism and promoting cooperation between SAs.
- **Going forward:** For businesses that only operate within a single Member State, and only process the personal data of data subjects residing in that Member State, interaction with the local SA under the Regulation will be similar to interaction with the local DPA under the Directive. Businesses that operate in more than one Member State will see a substantial change, as the One Stop Shop will mean that they predominantly interact with a single SA as their lead authority (rather than multiple DPAs).

The Directive

The Regulation

Art.28

Background and role: Each Member State must appoint one or more DPAs to oversee the implementation of the Directive, and to protect the rights and freedoms of data subjects.

Territorial scope: The DPA has oversight of processing activities taking place on the territory of its own Member State only.

Art.28(3)

Powers: Each Member State must provide its DPA with investigative powers, the power to intervene, and the power to initiate legal proceedings.

Art.29

Cooperation among DPAs: DPAs are obliged to cooperate with one another to the extent necessary to perform their duties.

The WP29: The WP29 comprises representatives of the DPAs, and serves in an advisory capacity.

The 'One Stop Shop': Under the Directive, a business is subject to enforcement by the local DPA of each Member State in which it operates.

The Consistency Mechanism: Under the Directive, DPAs can (and frequently do) adopt enforcement positions that differ from the positions adopted by other DPAs. This means that businesses face inconsistent compliance obligations across the various Member States.

Art.51

Background and role: Each Member State must appoint one or more SAs to oversee the application of the Regulation, and to protect the rights and freedoms of data subjects.

Territorial scope: The SA is only entitled to exercise its powers in its own Member State but, under the One Stop Shop, the SA's regulatory actions may affect processing that occurs in other Member States.

Art.58

Powers: The Regulation grants each SA the power to enforce the Regulation, to investigate breaches of the Regulation, and to initiate legal proceedings.

Art.60

Cooperation among SAs: The SAs must provide one another with mutual assistance in the performance of their duties and may carry out joint operations.

Art.68-76

The EDPB: The EDPB is a new EU body with legal personality and power to make binding decisions on enforcement. It also has a range of other tasks including an advisory role.

Art.56

The 'One Stop Shop': Where a business is established in more than one Member State, it will have a 'lead authority', determined by the place of its 'main establishment' in the EU (i.e., the place where the main processing activities take place). The 'lead authority' effectively regulates that business across all Member States. Businesses that are established in only one Member State but have processing activities that impact data subjects in other Member States will also have a 'lead authority'.

Art.63-67

The Consistency Mechanism: Where a processing activity affects data subjects in more than one Member State, the lead SA must consult with all other concerned SAs. If the SAs cannot agree the decision will be made by the EDPB.

Accountability



Why is this issue important for businesses? The Regulation will require businesses to implement measures to ensure that their processing activities comply with the Regulation, and demonstrate that compliance to SAs and data subjects.



Affected sectors: Businesses in all sectors will need to review their compliance programs and, where necessary, take remedial action.

- **Accountability in general:** The Regulation will require controllers to implement policies and procedures to ensure compliance with the Regulation. In addition, controllers must demonstrate their compliance. Elements of a compliance program include (but are not limited to):
 - appointing a DPO (if required);
 - maintaining internal records;
 - implementing robust information security measures (see page 24); and
 - conducting data protection by design and DPIAs (see page 20).
- **Data protection registrations:** Under the Directive, controllers are required to register their processing activities with the relevant DPA. The level of detail required varies between Member States.
- **Data Protection Officers:**
 - **Under the Directive:** There is no obligation to appoint a data protection officer (“DPO”) under the Directive, although some businesses choose to do so. In addition, some Member States (e.g., Germany and Sweden) have provided an exemption from the obligation to register, if a DPO is appointed and maintains records of the controller's processing activities.
 - **Under the Regulation:** A DPO must be appointed where:
 - the controller is in the public sector; or
 - its core activities involve systematic monitoring on a large scale; or
 - its core activities involve large scale processing of sensitive data; or
 - it is required by Member State law.

The Regulation will abolish the registration requirement, and replace it with an obligation to maintain internal records of data processing activities. The Regulation sets out a list of information that must be included in these internal records and, in many cases, the list is similar to the equivalent national registration requirements under the Directive.

- **Going forward:** Businesses should:
 - **Review their existing compliance programmes.** To the extent that a business's existing compliance programme does not fully address the requirements of the Regulation, that programme should be updated and expanded as necessary.
 - **Ensure that they have clear records of all of their data processing activities.** If this information has already been collated (e.g., as the result of a recent registration project) then producing internal records is likely to be straightforward.
 - **Identify a suitable person to fulfil the role of the DPO (if required)** and ensure the DPO has sufficient resources and independence to adequately perform his or her duties.

The Directive

The Regulation

Art.5 & 24

Accountability: Controllers have direct compliance obligations under the Directive, but the concept of accountability is not directly addressed.



Accountability: Controllers must be able to ensure and demonstrate, including through the adoption and implementation of appropriate data protection policies, that their processing activities comply with the requirements of the Regulation.



Art.18 & 19

Registration: Under the Directive, the national laws of most Member States require controllers (and in some cases processors) to register with the relevant DPA by providing information about their processing activities. This requirement, the applicable exemptions, and the precise contents of the registration application vary across the Member States.



Art.30

Internal records: In place of registrations, controllers and processors must maintain (and make available to SAs upon request) internal records that cover all of their data processing activities, including:

- details of the controller and the DPO;
- the purposes of those processing activities;
- the categories of personal data and data subjects;
- details of any recipients of the data;
- applicable retention periods; and
- security measures.



Recital 49; Art.18

Appointment, position and role of a DPO: The Directive provides very little substance on the role of DPOs. It states that the role of the DPO is to ensure the internal application of applicable data protection law within a business. It also explains that DPOs can be internal or external appointments, and that the DPO must function independently of the controller. However, the precise role of the DPO varies across the Member States.



Art.37-39

Appointment of a DPO: Corporate groups may appoint a central DPO. The DPO:

- must have expert knowledge of data protection law and be able to perform the DPO role; and
- may be an employee or an external contractor.

Controllers and processors must designate a DPO where:

- the processing is by a public body;
- the core activities involve regular and systematic monitoring of data subjects on a large scale; or
- the core activities involve large-scale processing of data in the special categories.

In other cases, DPO appointment is not mandatory.

Position of the DPO: The DPO must operate independently and not take instructions from the business as to the exercise of his or her functions. The DPO must also report to the management of the business.

Role of the DPO: The DPO must:

- advise the business on its compliance obligations;
- monitor compliance with those obligations;
- act as a contact point for data subjects;
- provide advice on the implementation of data protection by design and DPIAs (see page 20); and
- act as a contact point for SAs.



Information Notices



Why is this issue important for businesses? In order to give effect to the rights of data subjects (see page 38), all businesses have a duty to provide certain minimum information about their data processing activities to data subjects.



Affected sectors: Businesses that act as controllers will have to comply with the requirement to provide notices to data subjects.

- **The Directive:** The Directive specifies a minimum set of information to be provided by controllers to data subjects. Some Member States have gone beyond the minimum requirements. Consequently, the precise information that must be provided in an information notice varies from one Member State to another. Businesses operating in several Member States are required to assess their notice obligations on a country-by-country basis.
- **The Regulation:** The Regulation sets a higher standard of notice than the Directive, by adding a number of new fields of information that must be provided in all information notices.
 - *The primary advantage for businesses* of the approach in the Regulation is that a single notice likely will be sufficient in all Member States (although translations into the relevant local language will still be necessary).
 - *The primary disadvantage for businesses* of the approach in the Regulation is that notices will have to be more detailed. This is a particular challenge for businesses that frequently share data intra-group, without tight restrictions on the purposes for which other group entities may use those data.
- **Penalties for failing to provide a valid information notice:** The Regulation will increase both the details to be provided in these notices and the penalties for failing to comply (see page 12). Failure to provide a valid information notice may attract a fine of up to **€20 million or 4% of annual worldwide turnover**, whichever is greater.
- **Going forward:** Businesses currently have an obligation to provide notice of their processing activities to data subjects, but not all such notices are compliant with the existing law. Before the Regulation comes into force, businesses should take the opportunity to review their existing information notices and identify any missing details that will need to be provided under the Regulation. Although this is likely to require substantial effort, businesses can build on their existing information notices, as the basic information required under the Directive is also required under the Regulation.
- **Icons:** The Regulation allows the controller to supplement their information notices with standardised, machine-readable icons, and empowers the Commission to develop standardised icons.

The Directive

The Regulation

Art.10 & 11

General principle: Controllers must provide certain minimum information to data subjects.

Format: There are no specific requirements concerning the format in which information notices must be provided.

Content: Information notices must:

- identify the controller (and any representative);
- state the purposes of the processing;
- identify recipients of the data;
- briefly explain the rights of access and rectification (see page 38); and
- provide any further information reasonably necessary to guarantee fair processing.

If the data are obtained directly from the data subject, the notice must state whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply.

If the data are not obtained directly from the data subject, the notice must list the categories of data being processed.

Timing: Where data are collected from the data subject, there is no specific timing requirement for the notice, but DPAs typically take the view that it must be provided at the point of collection.

Where data are not collected from the data subject, notice should be provided:

- at the time of collection; or
- in the event of a disclosure to a third party, no later than the first disclosure.

Exemptions: Notice does not need to be provided if the data subject already has the relevant information. Member States can create additional exemptions (e.g., where the processing relates to the detection or prevention of crime).

Where the data are not obtained from the data subject, notice is not required if:

- it is impossible or involves disproportionate effort;
- the processing is required by law; or
- an exemption applies (e.g., the processing is carried out for the purposes of national security, journalism, or artistic or literary expression).

Art.12 & 13

General principle: Controllers must provide certain minimum information to data subjects.

Format: Controllers are expected to:

- have transparent and easily accessible information notices; and
- provide information in an intelligible form, using clear and plain language, in particular, if the notice is addressed specifically to children.

Content: In addition to the requirements of the Directive, information notices under the Regulation must also provide:

- the identity and contact details of the DPO (if any);
- an explanation of the controller's legitimate interests, if the processing is based on those interests;
- the data retention period;
- a brief explanation of the rights to erasure and to object to processing (see page 38);
- the right to complain to the SA; and
- information on cross-border data transfers.

Where the personal data are not obtained directly from the data subject, the notice should also identify the source of the data.

Timing: Where data are collected from the data subject, the information notice should be provided at the point of collection.

Where data are not collected from the data subject, notice should be provided:

- before, or within a reasonable period after, collection, at the latest within one month;
- in the event of a disclosure to a third party, no later than the first disclosure; or
- at the first communication with the data subject.

Exemptions: Notice does not need to be provided if the data subject already has the relevant information.

Where the data are not obtained from the data subject, notice is not required if:

- it is impossible or involves disproportionate effort;
- the processing is required by law; or
- an exemption applies (e.g., the processing is carried out for the purposes of national security, journalism, or artistic or literary expression).

Data Protection by Design and by Default / DPIAs



Why is this issue important for businesses? These principles require businesses to take data protection issues into account from the start of any product design process and during the processing, and to properly assess the risks before launching any new types of process.



Affected sectors: All business sectors will be affected by these requirements.

- **Data protection by design:** Whenever a business adopts a new technology, product or service, it should do so in a way that ensures compliance with data protection obligations. Businesses should consider the entire life-cycle of the relevant processing activities, and plan for foreseeable uses of the new technology, product or service that may affect the data protection rights of data subjects. Businesses must implement mechanisms for ensuring that, by default, personal data are only processed insofar as necessary for the intended purposes, are not collected or kept beyond the minimum necessary for these purposes and are not made accessible to an indefinite number of individuals.
- **DPIAs:** DPIAs will be required for high risk processing to (i) assess the privacy risks to individuals related to a proposed data processing activity; and (ii) identify measures to address these risks and demonstrate compliance with the Regulation. Where a DPIA indicates that the processing is high risk and it is not possible to mitigate that risk, the controller will be required to consult the SA.
- **Privacy as a differentiator:** DPIAs provide a tangible tool to which a business can point, to demonstrate that it takes the privacy concerns of its customers seriously, and that it has appropriately addressed those concerns. This, in turn, can help that business to differentiate its products and services from those of its competitors and reassure its customers that their personal data will be processed safely and responsibly.
- **Limited economic impact:** Although the principles of data protection by design and by default, and the requirement to perform DPIAs, impose a clear administrative burden on businesses, the overall cost of these measures will often be limited, once internal systems and procedures have been implemented to aid management of these issues. The costs are likely to be offset by the long-term benefits of compliance, bearing in mind the potentially significant cost of non-compliance (see page 12).
- **Going forward:** Under the Regulation, businesses are legally required to: (i) take data protection requirements into account from the inception of any new technology, product or service that involves the processing of personal data; and (ii) conduct DPIAs where appropriate. These steps will need to be planned into future product cycles.

The Directive

The Regulation

Art.25

Privacy by design and by default – General Principle: The concepts of privacy by design and by default are not explicitly addressed in the Directive.

Data Protection by design and by default – General Principle: When designing a processing system, and when using that system to process data, controllers must implement appropriate technical and organisational measures to protect the rights of data subjects and ensure compliance with the Regulation. Businesses must ensure that, by default, data processing activities are limited to the minimum necessary for the purpose.

Art.35

DPIAs – General Principle: DPIAs are not explicitly addressed in the Directive, although several national DPAs recommend that a DPIA be undertaken in certain circumstances.

DPIAs – General Principle: The controller is required to perform a DPIA in the event that the relevant processing operations present high risks to the rights and freedoms of the data subjects. DPIAs are always required where the processing involves:

- systematic evaluation of personal characteristics, including Profiling, on which decisions concerning individuals that produce legal effects are made;
- processing special categories of data on a large scale; or
- systematic monitoring of a publicly accessible area on a large scale.

DPIAs – Scope: DPIAs are not explicitly addressed in the Directive.

DPIAs – Scope: The Regulation provides a non-exhaustive list of processing activities that require a DPIA. This list includes:

- systematic Profiling activities (see page 22);
- processing of information in the special categories; and
- large-scale surveillance in public areas.

SAs can add to this list, and can require controllers to carry out a prior consultation and a DPIA.

DPIAs – Content: The content of DPIAs is not explicitly addressed in the Directive, although some national DPAs have issued guidance, and the WP29 has issued DPIA frameworks for RFID applications and Smart Meters.

DPIAs – Content: A DPIA should contain:

- a description of the processing activities being assessed;
- an assessment of the risks to data subjects; and
- a description of the measures the controller will take to address these risks, including the safeguards, security measures and mechanisms that the controller will implement to ensure compliance with the Regulation.

Profiling



Why is this issue important for businesses? Increasingly, businesses Profile their customers. The Regulation increases the protection of data subjects against possible negative effects of such Profiling.



Affected sectors: This issue is of particular relevance to businesses that provide or use services related to online marketing, analytics, customer tracking and ad conversion.

- **Definition of 'Profiling':** Profiling means any automated processing of personal data to evaluate personal aspects subjects in particular their work performance, economic situation, health, behaviour, preferences, interests, reliability, location or movements. Examples of Profiling activities include forms of customer tracking and ad conversion measurement.
- **Technological advances:** One of the key drivers behind the Regulation is the need to adapt EU data protection law to the risks and opportunities created by technological developments. In particular, Profiling allows businesses to analyse and predict aspects of a data subject's behaviour (such as consumption habits, interests, preferences, etc.), in many cases without the data subject even being aware. While these developments have obvious advantages, they also carry inherent privacy risks, which the Regulation seeks to address.
- **Protection for data subjects:** The Regulation strengthens the protections available to data subjects against possible negative effects of Profiling by granting them a right not to be subject to decisions based solely on automated processing of their personal data, including Profiling, that produce 'legal effects' concerning them or significantly affect them, in limited cases.
- **The need for consent:** In practice, the only lawful basis for taking decisions based on Profiling that will be available to businesses in most circumstances will be the explicit consent of the data subject. The Regulation makes it more difficult for businesses to obtain valid consent (see pages 8 and 28). Consequently, lawful Profiling is likely to be substantially more difficult to achieve under the Regulation. For example, passive acquiescence of users to a general set of terms and conditions will not result in valid consent. Instead, it will be necessary to implement tick-boxes or similar mechanisms to secure the data subject's positive indication of consent to specific processing activities related to Profiling.
- **Going forward:** The impact of the Regulation's restrictions on Profiling on a given business will largely depend on how frequently that business engages in Profiling activities. For those businesses for which Profiling is a rare or occasional activity, it may simply be easier to cease such activities than to comply with the Regulation. Those businesses that regularly engage in Profiling activities will need to consider how best to implement appropriate consent mechanisms in order to continue these activities.

The Directive

The Regulation

Art.15

General concept: The Directive does not explicitly define or refer to the concept 'Profiling'. However, it does regulate a similar (though narrower) practice of 'automated individual decisions' that produce 'legal effects' on data subjects, or significantly affect them.



Art.22

General concept: The Regulation explicitly refers to "Profiling" as a type of automated individual decision-making and defines it as: "any form of automated processing or 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 natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

Restrictions on 'automated individual decision-makings': Data subjects have the right not to be subject to automated individual decision-making except if:

- the decision is taken in the course of the performance of, or entering into, a contract, provided that: (a) the request for entering into or perform the contract, lodged by the data subject, has been satisfied or (b) there are suitable measures in place to protect the data subject's legitimate interests; or
- the decision-making is authorised by a Member State law that provides suitable safeguards for the data subject's legitimate interests.



Restrictions on Profiling: Data subjects have the right not to be subject to decisions based solely on automated processing, including Profiling, that produce legal effects concerning them or similarly significantly affect them unless the decision:

- is necessary for the performance of, or entering into, a contract, between the data subject and a controller;
- is expressly authorised by an EU or Member State law to which the controller is subject and that provides suitable safeguards for the data subject's rights, freedoms and legitimate interests; or
- is based on the data subject's explicit consent.

Rights of data subjects: As part of the right of access to data (see page 38), data subjects have the right to obtain information on the logic involved in any automated processing of data concerning them.



Rights of data subjects: The information notice (see page 18) should inform data subjects about the existence of Profiling and, at least, include meaningful information about the logic involved, as well as the significance and the envisaged consequence of the Profiling.

Automated individual decision-making based on sensitive personal data: The Directive does not directly address automated individual decision-making based on sensitive personal data.



Automated processing of personal data in the specified categories: Profiling on the basis of sensitive personal data: Profiling performed on the basis of sensitive personal data generally require explicit consent of data subjects. (See the definition on page 9).

Data Breach Reporting



Why is this issue important for businesses? The Regulation introduces a general data breach reporting obligation.



Affected sectors: Any business that suffers a data breach will be subject to the new reporting requirements under the Regulation.

- **The Directive:** Under the Directive, there is no general obligation on businesses to notify data breaches either to DPAs or to the affected data subjects. (Although there are some sector-specific breach reporting obligations in other areas of EU law – e.g., for providers of electronic communications services, there is a reporting obligation under the e-Privacy Directive 2002/58/EC, as amended).
- **Consequences of non-compliance:** Businesses that fail to fulfil their data breach reporting obligations may be sanctioned by the SA with a fine of up to **€10 million or 2% of annual worldwide turnover**, whichever is greater.
- **Going forward:** Businesses will need to develop and implement a data breach response plan (including designating specific roles and responsibilities, training employees, and preparing template notifications) enabling them to react promptly in the event of a data breach.

Some Member States have implemented breach reporting obligations in their national laws (e.g., Austria, Germany and the Netherlands). Furthermore, the WP29 and certain local DPAs (e.g., Belgium, Denmark, Ireland and the United Kingdom) have issued guidance strongly urging businesses to voluntarily report serious data breaches.

- **The Regulation:** The Regulation will introduce a general data breach reporting obligation, requiring controllers in all sectors to inform the competent SA and, in certain cases, affected data subjects.

The purpose of implementing a general data breach reporting requirement is to: (i) make it easier for SAs to exercise their supervisory functions (see page 14); (ii) enable affected data subjects to take measures to mitigate the risks related to the data breach (e.g., cancel affected credit cards); and (iii) motivate businesses to implement robust information security measures in order to avoid data breaches.

Information security measures will need to be re-assessed to ensure that data breaches can be detected and managed promptly. Businesses should also consider implementing measures to ensure that any data that are subject to a breach are unintelligible to any person who is not authorised to access the data (e.g., by encrypting data wherever possible), as this may exempt the business from the obligation to report the breach to the affected data subjects, and may help prevent harm to the business's reputation.

Complying with the data breach reporting obligations in the Regulation will also entail a significant administrative burden for businesses, which may increase costs. On the other hand, the harmonisation of the data breach reporting obligation will allow businesses operating across multiple Member States to have one pan-EU data breach response plan.

The Directive

Concept: A data breach is any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, usually as the result of a breach of security.



Data breach reporting obligations generally: The Directive does not contain a general data breach reporting obligation. Some Member States have implemented data breach reporting obligations in their national law (e.g., Austria, Germany and the Netherlands). In other Member States, local DPAs have issued non-binding guidance in which they strongly recommend controllers to notify personal data breaches (e.g., Belgium, Denmark, Ireland and the UK).



Reporting breaches to the competent DPA: The Directive does not specify any requirements regarding the reporting of data breaches to DPAs.



Reporting breaches to affected data subjects: The Directive does not specify any requirements regarding the reporting of data breaches to affected data subjects.



The Regulation

Concept: A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, transmitted, stored or otherwise processed.



Art.33 & 34

Data breach reporting obligations generally: The Regulation introduces a general obligation to report data breaches:

- to the competent SA unless the breach is unlikely to be a risk to individuals; and
- to the affected data subjects (if the breach is likely to result in a high risk to the rights and freedoms of data subjects).

If the breach is suffered by a processor, the processor must report it to the controller immediately after it is discovered.



Reporting breaches to the competent SA:

- **Timing:** Data breaches must be reported to the relevant SA without undue delay and, where feasible, no later than **72 hours** after being discovered. If it is not possible to notify the SA within 72 hours, this delay must be justified to the SA.
- **Content:** The report to the SA should include: (i) a description of the nature of the data breach (including the number and categories of data subjects and volume of data affected); (ii) the name and contact details of the DPO or other contact point; (iii) a description of consequences of the breach; and (iv) a description of the measures proposed or taken to address the breach.
- **Exemptions:** None.



Reporting breaches to affected data subjects:

- **Timing:** Data breaches must be reported to the affected data subjects without undue delay.
- **Content:** Data subjects should be told about the nature of the data breach, and given the contact details of the DPO or other contact point, and informed of any recommended measures to mitigate possible adverse effects of the breach.
- **Exemptions:** It is not necessary to inform affected data subjects in some cases, e.g., if the controller can demonstrate, to the satisfaction of the SA, that it has implemented appropriate information security measures that render the data unintelligible to any person not authorised to access it (e.g., the lost data are protected by encryption) or taken measures to mitigate the high risk for data subjects.



Obligations of Processors



Why is this issue important for businesses? Unlike the Directive (which generally places direct compliance obligations only on controllers), the Regulation will impose direct compliance obligations on processors as well.



Affected sectors: This issue primarily affects businesses that act as processors, but it may also affect any business that engages a processor to process data on its behalf.

- **The Directive:** Under the Directive, the primary obligation to comply with EU data protection law falls on controllers. If a DPA takes any enforcement action, it does so against the controller. The controller is required to impose certain compliance obligations on any processor it appoints, in a binding contract, but the DPA generally does not have direct enforcement powers against the processor.
- **The Regulation:** Rather than relying on controllers to contractually flow down compliance obligations to processors, the Regulation will impose a number of obligations directly on processors. These direct obligations include:
 - maintaining records of processing activities;
 - cooperating with the relevant SA;
 - implementing appropriate security measures;
 - informing the controller in the event of a data breach; and
 - complying with the requirements of the Regulation regarding cross-border data transfers (see page 32).
- **Contractual obligations:** Much like the Directive, the Regulation will require that the outsourcing of data processing activities by a controller to a processor is governed by a written data processing agreement. Whereas the Directive does not specify the content of this data processing agreement, the Regulation mandates in detail the terms that must be included in such an agreement.
- **Penalties for failure to comply:** Because processors will have direct compliance obligations under the Regulation, they will also face penalties for non-compliance. Deliberate or negligent breach by a processor of its obligations may attract a fine of up to **€20 million or 4% of annual worldwide turnover**, whichever is greater.
- **Going forward:** The Regulation is likely to substantially impact both processors and controllers that engage processors:
 - The increased compliance obligations and penalties for processors are likely to result in an increase in the cost of data processing services.
 - Negotiating data processing agreements may become more difficult, as processors will have a greater interest in ensuring that the scope of the controller's instructions is clear.
 - Processors and controllers will have to review their existing data processing agreements, to ensure that they have met their own compliance obligations under the Regulation.

The Regulation also explicitly states that a processor will be considered a joint controller in the event that it processes personal data other than in accordance with the instructions of the controller.

The Directive

The Regulation

Art.4(1)(a)

Application of the law: Under the Directive, EU data protection law applies directly to **controllers**.



Art.3(1)

Application of the law: Under the Regulation, EU data protection law applies directly to **controllers and processors**.



Art.17

Appointing a processor: A controller must appoint a processor under a written data processing agreement.



Art.28-30

Appointing a processor: A controller must appoint a processor under a written data processing agreement.



Content of data processing agreements: The data processing agreement must specify that the processor shall:

- act only on instructions from the controller; and
- implement appropriate technical and organisational information security measures.

Many Member States have implemented additional requirements that go beyond the requirements of the Directive.



Content of data processing agreements: The data processing agreement must specify that the processor shall:

- act only on instructions from the controller;
- impose a duty of confidentiality on relevant staff;
- implement the necessary security measures;
- subcontract processing activities only with the controller's prior permission;
- insofar as possible, make arrangements to enable the controller to respect the rights of data subjects (see page 38);
- assist the controller in complying with its obligations regarding data security and consultation with SAs;
- return all relevant personal data to the controller after the end of the processing and not process the relevant personal data further; and
- make available to the controller and the relevant SA all necessary information regarding the processor's data processing activities.



Art.30-33; 36-37 & 44

Direct legal obligations of processors: The Directive does not impose direct legal obligations on processors.



Direct legal obligations of processors: The Regulation requires processors to:

- maintain records of their processing activities;
- co-operate with the SA;
- implement appropriate technical and organisational information security measures;
- inform the controller immediately after discovering a data breach; and
- comply with the restrictions regarding cross-border data transfers.



Direct enforcement against processors: EU data protection law cannot be enforced directly against processors under the Directive.



Direct enforcement against processors: The Regulation will be enforced by SAs directly against processors.



Processing Conditions



Why is this issue important for businesses? A '*processing condition*' is a legal basis for processing personal data. Businesses must satisfy at least one processing condition for each data processing activity they undertake.



Affected sectors: Businesses in all sectors will need to ensure that they have valid processing conditions for their data processing activities.

- **The Directive:** Under the Directive, all processing activities (including collecting, reviewing, deleting or merely storing personal data) require a 'processing condition'. A processing condition is a lawful ground on which personal data may be processed, and these are set out in the Directive (see page 29). A narrower set of processing conditions applies to the processing of sensitive personal data.
- **The Regulation:** Under the Regulation, processing conditions are more onerous. In particular, consent will become significantly harder to rely on (see also the revised definition of consent, which requires a statement or clear affirmative action from the data subject, discussed on page 8).
- **Conditions for consent:** Where consent is given in a document that also concerns other matters (e.g., a set of website terms and conditions) the Regulation requires that the consent request is presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language (Art.7(2)). As a result, businesses will not be able to rely on a standard set of contractual terms to obtain consent for the processing of personal data. The Regulation also requires that it is as easy to withdraw consent as it was to give it.
- **'Freely given':** Under the Regulation, consent may not be considered to be freely given if the performance of a contract is made conditional on the data subject's consent to the processing of his or her personal data that is not necessary for the performance of the contract.
- **Specific protection for children:** The Regulation sets forth more stringent conditions for the processing of children's data. Businesses offering information society services to children (below the age of 16, or a lower age provided by Member State law that cannot be below 13) that want to rely on consent for the processing of personal data will, for example, be required to obtain consent or authorisation from the person holding parental responsibility over the child.
- **Sensitive personal data:** The Regulation broadens the concept of sensitive personal data by adding genetic data and biometric data to the categories of data that are deemed to be sensitive. On the other hand, the Regulation provides additional grounds for the processing of such data by allowing the processing of sensitive personal data where it is necessary for reasons of substantial public interest, as well as for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, provided that additional safeguards (including pseudonymisation) are put in place.
- **Going forward:** Businesses will need to carefully consider whether they have a lawful processing condition for all of their data processing activities. Where no processing condition applies, businesses will need to determine whether: (i) another processing condition might be available (e.g., by obtaining consent from affected data subjects); or (ii) that processing activity should cease.

The Directive

Art.7(b-e)

General processing conditions: Personal data may be processed if the processing is necessary:

- for the **performance of a contract** to which the data subject is party, or into which the data subject is seeking to enter;
- for **compliance with a legal obligation**;
- to protect the **vital interests** of the data subject;
- for the performance of a task carried out in the **public interest** or to exercise an official authority vested in the data controller or in a third party; or
- for the **legitimate interests** of the data controller or a third party, except where such interests are overridden by the interests or the rights and freedoms of the subject.



Art.7(a)

Consent: Consent is a valid processing condition if the data subject has 'unambiguously' given his or her consent.



Art.8(1) & 8(2)

Consent to process sensitive personal data: The processing of sensitive personal data usually requires the consent of the data subject.



Art.8(1)(b), (c) and (e) & 8(3)

Processing sensitive personal data: Sensitive personal data may be processed with the consent of the data subject or if the processing is necessary:

- for the purposes of applicable employment law;
- to protect the vital interests of the data subject or another individual;
- for the purposes of a legal claim;
- as it relates to data that have been deliberately made public by the data subject;
- for preventive medicine, medical diagnosis, provision of care or treatment or the management of healthcare services; or
- for additional grounds created by Member States in their national laws.



The Regulation

Art.6(1)(b-f) & 6(3)

General processing conditions: Personal data may be processed if the processing is necessary:

- for the **performance of a contract** to which the data subject is party, or into which the data subject is seeking to enter;
- for **compliance with an EU legal obligation**;
- to protect the **vital interests** of the data subject or another individual;
- for the performance of a task carried out in the **public interest** or to exercise an official authority vested in the data controller; or
- for the **legitimate interests** of the data controller or a third party, except where such interests are overridden by the interests or the rights and freedoms of the subject, in particular if the data subject is a child.

Art.6(1)(a) & 7

Consent: To be valid, consent must relate to the processing of personal data for a specified purpose. Where consent is obtained in a document that also concerns another matter, the consent must be distinguishable from that other matter. Consent may be considered to be invalid where the performance of a contract is made conditional upon giving consent to the processing of personal data which is not necessary for the performance of the contract. It is up to the data controller to demonstrate that consent was given.

Art.9(1) & 9(2)(a)

Consent to process sensitive personal data: The processing of sensitive personal data is prohibited without the explicit consent of the data subject.

Art.9(2)(b), (g), (h) and (j)

Processing sensitive personal data without consent: In addition to consent and the other conditions set out in the Directive, the grounds for processing sensitive personal data include cases where the processing:

- is necessary for the purposes of applicable social security and social protection law;
- is carried out for reasons of substantial public interest, on the basis of EU or Member State law, subject to appropriate protections;
- is necessary for reasons of public interest in the area of public health, on the basis of EU or Member State law, subject to appropriate protections; or
- is necessary for archiving purposes in the public interest or for historical, statistical or scientific purposes, subject to appropriate protections.

Anonymisation and Pseudonymisation



Why is this issue important for businesses? In many cases, businesses can use data that would otherwise be subject to EU data protection law if those data are anonymised, so that data subjects are no longer identifiable.



Affected sectors: This issue is particularly relevant to businesses that re-purpose or publish existing data (e.g., 'big data' analytics, CROs, data aggregators, etc.).

- **Background:** In some cases a business may want to use data about people, without needing to identify the data subjects to whom that data relate (e.g., in clinical trials, or statistical analysis). Structuring data in such a way that they do not enable the direct identification of data subjects can help businesses meet their data protection obligations or even remove that data from the scope of the Regulation entirely. There are two ways to achieve this:
 - **'Anonymous data'** are data that do not relate to an individual or data rendered anonymous in such a way that the data subject is no longer identifiable. 'Anonymous data' are not personal data and are not subject to the requirements of EU data protection law.
 - **'Pseudonymous data'** are data that are 'coded' (i.e., certain information, such as a data subject's name and address, is replaced with pseudonyms) in such a way that the data cannot be attributed to a particular data subject without the use of additional information (i.e., a 'key' that can re-identify data subjects from the data). The 'key' necessary to identify data subjects from the coded data must be kept separately, and should be subject to technical and organisational security measures to prevent inadvertent re-identification of the coded data. The use of pseudonymous data can reduce the risks for data subjects related to the processing of their personal data and help controllers and processors meet their data protection obligations under the Regulation.
- **Pseudonymisation as a data protection safeguard:** The Regulation refers to pseudonymisation as one of the possible measures to:
 - ascertain that further processing of data for another purpose is compatible with the purpose for which the data was initially collected;
 - ensure an appropriate level of information security;
 - meet data protection by design obligations (see page 20); and
 - ensure that the data minimisation principle is respected when processing data for archiving in the public interest, for scientific or historical research purposes, or statistical purposes.
- **Processing not requiring identification:** Under the Regulation, businesses will not be required to maintain, acquire or process additional information allowing them to identify data subjects merely to be able to comply with the Regulation (e.g., handle data subjects' requests) if such identifiable information is not necessary to achieve the purpose of the data processing.
- **Going forward:** Currently, national DPAs have differing approaches to anonymisation and pseudonymisation, and different criteria for determining whether data are truly anonymised or pseudonymised. Compliance with these divergent guidelines is often difficult for businesses that process anonymous or pseudonymous data in multiple Member States. EU-wide guidelines are expected to be produced under Art.38 of the Regulation once it enters into force, unifying the current disparate approaches.

The Directive

The Regulation

Recital 26

Anonymous data: The Directive recognises that the rules that apply to personal data do not apply to data that are anonymised (i.e., data which do not relate to an individual or data rendered anonymous in such a way that the data subject is no longer identifiable).



Recital 26

Anonymous data: The Regulation recognises that the rules that apply to personal data do not apply to data that are anonymised (i.e., data which do not relate to an individual or data rendered anonymous in such a way that the data subject is no longer identifiable).



Definitions: The concepts of anonymous data and pseudonymous data are not explicitly defined in the Directive.



Art.4

Definitions:

- 'Anonymisation' is not defined.
- 'Pseudonymisation' is processing data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, which is kept separately and is subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.



Re-identification of anonymous and pseudonymous data: The Directive is silent on this issue.



Art.11

Re-identification of anonymous and pseudonymous data: Businesses are not obliged to collect further information in order to identify data subjects who are otherwise not identifiable.



Cross-Border Data Transfers



Why is this issue important for businesses? The Directive and the Regulation both restrict the ability of businesses to transfer personal data out of the EEA. For any business with multinational operations, this is a significant issue.



Affected sectors: This issue affects all businesses that transfer personal data out of the EEA and, increasingly, businesses that use cloud platforms and remote IT services.

- **The Directive:** Under the Directive, businesses are prohibited from transferring personal data out of the EEA unless:
 - the transfer is to an Adequate Jurisdiction;
 - the transfer is made pursuant to a mechanism that ensures an adequate level of protection (e.g., Model Clauses); or
 - a derogation applies.
 - **The Regulation:** Under the Regulation, the existing transfer restrictions will be preserved, but additional transfer possibilities are added. Prior notification or authorisation when using Model Clauses will no longer be required. Under the Regulation, data transfer restrictions will need to be complied with by controllers and processors.
 - **Adequate Jurisdictions:** The European Commission has the power to determine that a non-EU jurisdiction (and, under the Regulation, a territory or specified sector within such a jurisdiction) offers an adequate level of protection for personal data, based on that country's data protection laws and approach to enforcement. A current list of the Adequate Jurisdictions is provided in the Glossary (see page 42).
 - **Model Clauses:** Transfers of personal data out of the EEA may also be made based on Model Clauses that cover:
 - transfers from a controller in the EU to a controller outside the EEA; or
 - transfers from a controller in the EU to a processor outside the EEA.
- Although the WP29 has published proposals for a set of processor-to-processor Model Clauses, no such clauses have yet been approved by the Commission.
- **Derogations:** The Directive allows a number of derogations from the general prohibition on cross-border data transfers (e.g., where the data subject has unambiguously consented to the transfer). The Regulation retains these derogations, but also allows limited cross-border data transfers on the basis of the controller's legitimate interests (subject to strict conditions that restrict the usability of this new provision).
 - **Binding Corporate Rules:** BCRs are addressed separately on pages 34-35.
 - **Codes of conduct and certification mechanisms:** The Regulation also allows cross-border data transfers based on an approved code of conduct or certification mechanism, provided that the controller or processor in the third country commits to comply with the safeguards provided in the code or certification (see page 36).
 - **Going forward:** Businesses should review their data flows, and consider whether they have appropriate data transfer mechanisms in place. If not, it will be important to ensure that such transfer mechanisms are in place before the Regulation comes into force.

The Directive

The Regulation

Art.25

General prohibition: Transfers of personal data to a third country are prohibited unless that third country ensures an adequate level of protection.

Adequate Jurisdictions: The Commission can determine that a non-EU jurisdiction has adequate protections in place for personal data. Transfers to Adequate Jurisdictions do not require a separate transfer mechanism (such as Model Clauses).

Art.44 & 45

General prohibition: Transfers of personal data to a third country are prohibited unless that third country ensures an adequate level of protection.

Adequate Jurisdictions: Adequacy determinations made under the Directive will continue to apply under the Regulation.

Art.25

Model Clauses: Transfers of personal data to non-EU jurisdictions may lawfully be made on the basis of Model Clauses approved by the Commission under the Directive.

Approval of Model Clauses: Several Member States require DPA notification or approval prior to transfers made on the basis of Model Clauses.

Art.26

Derogations: Transfers of personal data to non-adequate jurisdictions are permitted where:

- the data subject has **unambiguously consented** to the transfer;
 - the transfer is necessary to perform or enter into a **contract** with the data subject;
 - the transfer is necessary to conclude a contract with a third party **in the data subject's interest**;
 - the transfer is in the **public interest**;
 - the transfer is necessary to **establish, exercise or defend legal claims**;
 - the transfer is necessary to protect the **vital interests** of the data subject; or
 - the transferred data came from a **public register**.
- These derogations are implemented inconsistently across the Member States.

Data Protection Seals: The Directive does not mention Data Protection Seals.

Art.46

Model Clauses: Model Clauses approved by the Commission under the Directive will remain a valid transfer mechanism under the Regulation.

Approval of Model Clauses: Transfers made on the basis of Model Clauses will not require any specific authorisation from SAs.

Art.49

Derogations: The derogations under the Directive will continue to apply. In addition, transfers that are not frequent or massive may take place where:

- the transfer is necessary for the **legitimate interests of the controller**; and
- the controller has, based on the circumstances surrounding the transfer, adduced **appropriate safeguards**, where necessary.

Art.42

Data Protection Seals: Cross-border data transfers may lawfully be made if both the data exporter and the data importer hold an approved code of conduct or certificate mechanism.

Binding Corporate Rules



Why is this issue important for businesses? Businesses that transfer personal data out of the EEA require a valid transfer mechanism. BCRs are limited to intra-group transfers, but allow greater flexibility than some other transfer mechanisms.



Affected sectors: This issue affects businesses that engage in large, intra-group cross-border transfers of personal data (e.g., multinational businesses, or IT service providers).

- **The Directive:** Under the Directive, BCRs are not formally recognised as a valid data transfer mechanism. Many Member States require additional DPA approval for transfers, even if BCRs have been adopted. BCRs were first made available to controllers, and later to processors.
 - the tasks of any data protection officer or any other person or entity in charge of monitoring compliance with the BCRs;
 - the complaint procedures;
 - the mechanisms by which the relevant entities' compliance with the BCRs will be checked;
 - the mechanisms for reporting and recording changes to the BCRs and reporting these changes to the relevant SA; and
 - the cooperation mechanism with the relevant SA to ensure compliance with the BCRs by any group entity.
- **The Regulation:** The Regulation explicitly recognises BCRs as a data transfer mechanism and is expected to make the adoption of BCRs a simpler task. Member States will no longer require data exporters to obtain additional approval from SAs for transfers based on BCRs. BCRs will remain available to both controllers and processors.
- **Key elements of BCRs under the Regulation:** The Regulation stipulates that BCRs must include: (i) a mechanism to make the BCRs legally binding on relevant group entities and their employees; (ii) a mechanism to grant enforceable rights to data subjects; and (iii) a document including:
 - the list of entities bound by the BCRs;
 - the data transfers covered by the BCRs;
 - the legally binding nature of the BCRs;
 - the general data protection principles applicable to transferred data, including data protection by design and by default and the requirements in respect of onward transfers to entities not bound by the BCRs;
 - the rights of data subjects and the means of exercising those rights;
 - the acceptance, by a group entity within the EU, of liability for any breaches of the BCRs committed by any group entity outside the EU;
- **Changes to the approval process:** Under the Directive, the BCR approval process was simplified but still involved discussions with multiple DPAs, each imposing slightly different procedural requirements. The Regulation will clarify and further streamline the BCR approval process, by: (i) setting out a consistent list of requirements that applies across the whole of the EU; and (ii) making approval of BCRs subject to the Consistency Mechanism (see page 14) rather than interpretation by national SAs, as is currently the case.
- **Going forward:** As noted above, the Regulation formally recognises BCRs as a lawful data transfer mechanism, and makes it easier for businesses to obtain approval from SAs of their BCRs. Once the Regulation comes into force, it is likely that there will be an increase in the number of businesses that seek to implement BCRs.

The Directive

The Regulation

Art.26

Availability: BCRs are available as a data transfer mechanism to both controllers and processors.

Existing BCRs: BCRs that have been approved by the relevant DPAs are, subject to the terms of any approval, a valid data transfer mechanism.

Formal recognition: BCRs are not explicitly recognised in the Directive as a valid data transfer mechanism. The WP29 has recognised the validity of BCRs as a data transfer mechanism, but implementation requirements vary from one Member State to another.

Art.26

Approval requirements: The current approval requirements for BCRs are based on WP29 recommendations, which set out the necessary components and features for BCRs to ensure an adequate level of protection for transferred data. These requirements have been interpreted differently by the different Member States, meaning that there is no single set of consistent, EU-wide requirements.

Content and structure: The required content and structure of BCRs is set out in several guidance documents produced by the WP29.

Art.46

Availability: BCRs remain available as a data transfer mechanism to both controllers and processors.

Existing BCRs: BCRs that have been approved under the Directive will continue to be a valid data transfer mechanism, until amended, replaced or repealed by the relevant SA.

Formal recognition: The Regulation explicitly recognises BCRs as a valid data transfer mechanism. Member States are not entitled to impose further authorisation requirements for transfers based on BCRs.

Art.47

Approval requirements: Under the Regulation, SAs must, in accordance with the Consistency Mechanism, approve BCRs that:

- are legally binding on and enforceable against every member of the data exporter's group that will receive the data, and their employees;
- expressly confer enforceable rights on data subjects; and
- fulfil the information requirements set out in the Regulation.

Member States are not permitted to impose further approval requirements.

Content and structure: The content and structure set out by the WP29 is slightly expanded in the Regulation. Current elements of the BCRs are further developed (e.g., the general data protection principles). Some new elements are added, in particular the existence of mechanisms for reporting to the relevant SA any legal requirements to which a group entity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the BCRs.

Seals, Certifications and Codes of Conduct



Why is this issue important for businesses? Seals, certifications and codes of conduct provide a way for businesses to demonstrate to their customers that they take their data protection compliance responsibilities seriously.



Affected sectors: All businesses will be able to apply for seals and certifications, to give data subjects confidence that those businesses are compliant with the Regulation.

- **Background:** Privacy seals and certifications typically consist of a badge or other recognition that organisations are entitled to display if their data processing activities satisfy certain criteria. Businesses can then publicly use the seal or certification to help assure customers that the business is taking a responsible approach to privacy requirements.

Codes of conduct are generally specific to particular industries or categories of data processing activities, and are often used by businesses to demonstrate compliance with industry best practice.

- **The Directive:** Privacy seals and certifications are not explicitly recognised in the Directive, although there is an existing privacy seal scheme, known as 'EuroPriSe', which is available on an EU-wide basis to companies in the IT sector.

The Directive creates a framework for the assessment of codes of conduct by national DPAs and the WP29 against compliance with the Directive and national implementing laws.

- **The Regulation:** The Regulation explicitly recognises privacy seals, and sets out a framework for the adoption by the European Commission of EU-wide rules relating to privacy seals and certifications.

Under the Regulation, associations and other bodies representing categories of data controllers or processors may submit codes of conduct to SAs for their review and approval. The SAs will register and publish approved codes of conduct.

The Regulation introduces the possibility to transfer personal data out of the EEA on the basis of approved codes of conduct or certification mechanisms with binding and enforceable commitments to apply appropriate safeguards.

- **Going forward:** Existing privacy seal schemes drawn up by Member States and the EuroPriSe scheme are expected to be harmonised after the Regulation. In the meantime, businesses should review the status of existing privacy seal certifications, review their compliance with the requirements of the Regulation, and if necessary, reapply under the revised rules.

The Regulation provides a framework for the adoption of EU-wide codes of conduct, rather than the current adoption system for codes of conduct, which predominantly occurs at a national level. The adoption of codes of conduct is therefore expected to become a more popular tool for businesses to demonstrate compliance with the Regulation.

The Directive

The Regulation

Art.42

Formal recognition: The Directive does not address seals or certifications. Some Member State DPAs, and EuroPriSe at a pan-EU level, have proposed privacy seal initiatives.

Formal recognition: The Regulation explicitly recognises and encourages the adoption of certification mechanisms and privacy seals at an EU level.

Seals and certifications: Because there is no specific EU-wide law governing the creation of privacy seals, a number of different approaches have been taken. For example:

- **EuroPriSe** – an EU-wide scheme, aimed at the IT sector.
- **National schemes** – e.g., the French DPA operates a privacy seal scheme, available to businesses that provide data protection training and auditing services, and to businesses that provide software and computer systems.
- **Private sector schemes** – several private sector organisations, such as TRUSTe and the EDAA, run privacy seal programmes.

Seals and certifications: The Regulation empowers accredited certification bodies, SAs and the EDPB to issue certifications. Certification approved by the EDPB may result in a common certification, the 'European Data Protection Seal'. The Commission may specify relevant requirements and technical standards to be taken into account for the data protection certification mechanism and seals.

Art.27

Codes of conduct: The Directive requires Member States and the Commission to encourage the drawing up of codes of conduct intended to help ensure compliance with EU data protection law.

Art.40

Codes of conduct: The Regulation requires Member States, SAs, the EDPB and the Commission to encourage the drawing up of codes of conduct intended to help ensure compliance with EU data protection law.

Approval of codes of conduct: The Directive states that codes of conduct “may” be submitted to the WP29 for review, but does not specify a formal approval process or requirements.

Approval of codes of conduct: Interested parties are entitled to submit draft codes of conduct to the competent SA for opinion and approval. If the draft code relates to processing activities in several Member States, the EDPB will opine on the code's compliance with the the Regulation. The EDPB's opinion is subsequently submitted to the Commission, who can decide to grant the code general validity within the EU.

Rights of Data Subjects



Why is this issue important for businesses? The Directive and the Regulation both grant rights to data subjects regarding the processing of their personal data. In order to give effect to these rights, businesses need to be aware of their compliance obligations.



Affected sectors: All business sectors will need to enable data subjects to exercise their rights.

- **The Directive:** Under the Directive, data subjects are guaranteed certain basic rights in relation to their personal data, including the following:
 - **The right to certain minimum information:** Data subjects are entitled to receive certain minimum information from the controller about the processing of their personal data (see page 18).
 - **The right of access:** Data subjects are entitled to a copy of their personal data, and information about the processing of those data, upon payment of a small fee (if applicable) and without delay.
 - **The right to object:** Data subjects are entitled to object to processing of their personal data that is performed: (i) in the public interest; (ii) on the basis of legitimate interests of the controller; or (iii) for the purposes of direct marketing.
 - **The right to rectification, erasure or blocking of data:** Data subjects may exercise these rights where the processing is not in compliance with the Directive.
- **The Regulation:** Under the Regulation, the rights of data subjects set out in the Directive continue to apply (subject to minor amendments and clarifications) and the following rights are added:
 - **The 'right to be forgotten':** Following the CJEU's decision in *Costeja v Google*, the Regulation introduces a right to be forgotten as part of the 'right to erasure'. Under this right, data subjects can request controllers that process their data to erase any links to, or copy or replication of, their data.
 - **The right to data portability:** Where the processing is based on consent or is necessary for the performance of a contract with the data subject, and the processing is carried out by automated means, the Regulation entitles data subjects to receive personal data concerning them in a structured, commonly-used and machine-readable format. They can also request, where technically feasible, that the controller send their personal data to another controller.
- **Class remedies:** Where a data subject considers that the processing of his or her personal data does not comply with the requirements of the Regulation, he or she has the right to lodge a complaint with an SA (Art.73). The Regulation also provides data subjects with a right to compensation for material or immaterial damages suffered (Art.77). In addition, data subjects have the right to mandate a non-profit organisation or association to lodge complaints on their behalf.
- **Going forward:** In general, the rights of data subjects are expanded under the Regulation. As a result, businesses will need to devote additional time and resources to ensuring that these issues are appropriately addressed. In particular, businesses that rely on legitimate interests as a processing condition (see page 28) will need to consider in advance how they will respond to data subjects who exercise the right to object to processing carried out on that basis.

The Directive

The Regulation

Art.10 & 11

The right to certain minimum information: Controllers are required to provide data subjects with certain minimum information about the processing of their personal data (see page 18).



Art.13-14 & 23

The right to certain minimum information: Controllers are required to provide data subjects with certain minimum information about the processing of their personal data (see page 18).



Art.12

The right of subject access: Data subjects have a right to obtain from the controller, without excessive delay or expense:

- a copy of their personal data processed by or on behalf of the controller;
- the purposes of the processing;
- the recipients to whom the data are disclosed;
- information on the source of the data; and
- an explanation of the logic involved in any automatic processing of their personal data.



Art.15-17

The right of subject access: Data subjects have a right to obtain from the controller confirmation as to whether their personal data is being processed. Where such data are being processed, data subjects have the right to access the data, to obtain certain information regarding the processing of their personal data, and to obtain a copy of their personal data processed.



The right to rectification: Data subjects have a right to obtain the rectification of their personal data that are inaccurate, and the completion of personal data that are incomplete.



The right to rectification, erasure or blocking of data: Data subjects have a right to obtain from the controller the rectification, erasure or blocking of their data if the controller's processing activities are not compliant with the Directive (e.g., because the data are outdated or incomplete).



The right to erasure (including the 'right to be forgotten'): Data subjects have a right to erasure of their data for one of the following reasons:

- the data are no longer needed for their original purpose;
- the processing is based on consent, and the data subject withdraws that consent;
- the data subject exercises the right to object;
- a court holds that the data must be erased;
- the processing is unlawful;
- the data must be erased in order to comply with a legal obligation to which the controller is subject; or
- the data have been collected in relation to the offering of information society services to a child in accordance with Art.8(1).



The right to data portability: The Directive does not address this issue.



The right to data portability: The Regulation includes a right for data subjects to transfer their data to another data controller.



Art.14

The right to object: Where the controller's legal basis for processing the personal data is either that the processing is in the public interest, or in the legitimate interests of the controller, the data subject may object to that processing on *compelling legitimate grounds*.



Art.21(1) & (2)

The right to object: Where the controller's legal basis for processing the personal data is either that the processing is in the public interest or is necessary for the purpose of the legitimate interests of the data controller, the data subject may object to that processing unless the controller demonstrates compelling legitimate grounds for the processing.



Areas Remaining Unharmonised



Why is this issue important for businesses? Although the Regulation will largely harmonise data protection law across all Member States, there remain a number of areas in which businesses may face different requirements in each Member State.



Affected sectors: All businesses that operate in more than one Member State may be affected by the areas of law that will remain unharmonised under the Regulation.

- **The Directive:** Under the Directive, Member States have broadly similar data protection laws, but there remain significant differences between the relevant national laws. There are two key reasons for this:
 - There are issues that affect data protection, but fall outside the scope of the Directive. For example, the issue of national security falls outside the EU's legislative competence, and so each Member State takes its own approach to the question of what processing activities are necessary for national security (and are therefore exempt from the provisions of the Directive).
 - Even where the Directive addresses a particular issue, Member States have often implemented the requirements of the Directive differently. For example, the Directive sets out a minimum set of fair processing information to be provided to data subjects (see page 18) but Member States are free to insist on additional requirements.For these reasons, businesses currently face inconsistent data protection compliance requirements across the EU.
- **The Regulation:** Under the Regulation, the first issue identified above remains largely unchanged, as the limits on the EU's legislative competence have not changed. However, because the Regulation removes the need for national implementation, the second issue will (for the most part) fall away, resulting in a more consistent set of data protection compliance obligations across the EU.
- **Examples of areas remaining unharmonised:** Notwithstanding the greater harmonisation introduced by the Regulation, there will still be several issues that differ from one Member State to another. For example:
 - **National Security (Art.2(2)(a)):** Data processed for the purposes of the national security of a Member State are exempt from the Regulation. Member States have different conceptions of national security.
 - **Journalism and freedom of expression (Art.80):** The concepts of 'journalism' and 'freedom of expression' vary from one Member State to another (although Recital 121 of the Regulation states that 'journalism' should be interpreted broadly).
 - **Employment law (Art.82):** Member States may adopt more specific rules regarding the processing of personal data in an employment context.
 - **Professional secrecy laws (Art.84):** Some Member States have laws on professional secrecy that prevent the processing of certain data, even where the Regulation would otherwise permit that processing.
 - **Laws on interception of communications:** Member States have interception laws under the e-Privacy Directive 2002/58/EC as amended by Directive 2009/136/EC.
- **Going forward:** Although the Regulation increases harmonisation of data protection law across the EU, there remain areas in which the applicable requirements vary among the Member States. Businesses should keep these areas in mind when reviewing their obligations under the Regulation.

The Directive

The Regulation

Art.3

Member States retain discretion in some areas: Member States retain the flexibility to create exemptions to certain requirements of the Directive.



Art.2

Member States retain discretion in some areas: Although the Regulation introduces greater harmonisation, Member States still retain discretion in a number of areas.



Art.3, 9 & 13

Issues governed by national law: Under the Directive, exemptions and derogations, the scope of which is governed by national law, include the following:

- purely personal or household activity;
- journalistic purposes, and artistic or literary expression;
- national security, defence and public security;
- the prevention, investigation, detection and prosecution of criminal offences;
- important national economic interests;
- protection of data subjects;
- employment law; and
- professional secrecy laws.



Art.2, 23, 85, 87-88 & 90

Issues that continue to be governed by national law: Under the Regulation, the data processing which is governed by national law includes the following:

- national security;
- exclusively personal or household activity;
- the prevention, investigation, detection or prosecution of criminal offences;
- important national economic interests;
- protection of data subjects;
- journalism and freedom of expression, and artistic or literary expression;
- national identification numbers and general identities;
- employees' data; and
- professional secrecy laws.



Art.8, 18-19 & 24

Issues governed by national law: Under the Directive, examples of issues governed by national law include:

- *Sensitive personal data* – Member States retain some flexibility to lay down additional exemptions to the prohibition on processing sensitive personal data.
- *Registration with the local DPA* – Member States retain considerable flexibility in relation to exemptions from registration and the content of registration forms.
- *Sanctions* – Member States determine the sanctions to be imposed for breaches of national data protection law.



Art.15 & 83-84

Issues no longer governed by national law: Under the Regulation, examples of issues that will no longer be governed by national law include:

- *Sensitive personal data* – the conditions for processing sensitive personal data are harmonised under the Regulation.
- *Registration with the local SA* – registration will no longer be required under the Regulation (see page 16).
- *Sanctions* – Member States will still be required to lay down rules on the application of sanctions, but the sanctions themselves will be harmonised (excluding criminal sanctions).



Glossary

The following terms and abbreviations are used in this Guide:

- **'Adequate Jurisdictions'** – those jurisdictions that have been formally recognised by the Commission as providing an adequate level of data protection (i.e., Andorra, Argentina, Canada (for commercial entities subject to the Personal Information and Protection of Electronic Documents Act), the Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay).
- **'BCRs'** – Binding Corporate Rules (see page 34).
- **'CJEU'** – the Court of Justice of the European Union.
- **'Codes of Conduct'** – codes to which companies adhere in order to demonstrate compliance with their data protection obligations (see page 36).
- **'Commission'** – the European Commission (an EU institution).
- **'Consistency Mechanism'** – the mechanism by which national SAs are required to achieve consistent decisions across the EU under the Regulation (see page 14).
- **'controller'** – the entity that determines the purposes for which and means by which personal data are processed (see page 9).
- **'Council'** – the Council of Ministers of the European Union (an EU institution).
- **'CROs'** – Clinical Research Organisations.
- **'data breach'** – any accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data, usually as the result of a breach of security.
- **'data exporter'** – a controller or processor that transfers personal data out of the EEA.
- **'data importer'** – a controller or processor outside the EEA that receives personal data from the data exporter.
- **'data subject'** – the individual to whom personal data relates (see page 9).
- **'DPA'** – a Data Protection Authority under the Directive (see page 14). (The Directive uses the term 'Supervisory Authority' but most Member States, and the WP29, use the term 'DPAs' (when using English)).
- **'DPIA'** – Data Protection Impact Assessment (see page 20).
- **'DPO'** – Data Protection Officer (see page 16).
- **'EDAA'** – the European Digital Advertising Alliance.
- **'EDPB'** – the European Data Protection Board (an EU-level body created under Section 3 of Chapter VII of the Regulation that will oversee implementation and enforcement of the Regulation and issue guidance).
- **'EDPS'** – the European Data Protection Supervisor (an independent supervisory authority tasked with ensuring that EU institutions abide by the requirements of EU data protection law).
- **'EEA'** – the European Economic Area (which is made up of the EU Member States, plus Iceland, Liechtenstein and Norway).
- **'Member States'** – the Member States of the European Union (i.e., Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK).
- **'Model Clauses'** – the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries (note that there are several versions).
- **'Parliament'** – the Parliament of the European Union (an EU institution).
- **'personal data'** – information relating to an identified or identifiable individual (see page 9).
- **'processing'** – any operation that is performed upon personal data (see page 9).
- **'processor'** – an entity that processes personal data on behalf of the controller (see pages 9 and 26).
- **'Profiling'** – automated processing intended to evaluate information about a person or to analyse or predict his or her behaviour (e.g., performance at work, location or preferences).
- **'Regulation'** – the EU General Data Protection Regulation (see page 3).
- **'SA'** – a Supervisory Authority under the Regulation (see page 14).
- **'sensitive personal data'** – personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life. The Regulation adds genetic data and biometric data for the purpose of uniquely identifying a natural person, sexual orientation and criminal convictions or related measures (see page 9).
- **'WP29'** – the Article 29 Working Party (an advisory body comprising representatives of the DPAs from each of the 28 EU Member States and the EDPS).

Our Privacy Leaders



Lisa J. Sotto, Partner in the New York office of Hunton & Williams
+1 (212) 309 1223; lsotto@hunton.com

Lisa is the global head of the Privacy and Cybersecurity team and is based in the firm's New York office. She was named among *The National Law Journal's* "The 100 Most Influential Lawyers in America," and was rated the "No. 1 privacy expert" in all surveys by *Computerworld* magazine. She was ranked as a "Star Individual" for Privacy and Data Security by Chambers and Partners. Appointed by Secretaries Johnson and Napolitano, Lisa serves as Chairperson of the US Department of Homeland Security's Data Privacy and Integrity Advisory Committee.



Aaron P. Simpson, Partner in the London office of Hunton & Williams
+44 (0)20 7220 5612; asimpson@hunton.com

Aaron is a partner in the firm's London and New York offices. He has more than 10 years of experience assisting clients with a broad range of complex privacy and cybersecurity matters, including US and international privacy and data security requirements and the remediation of large-scale data security incidents. Aaron was ranked as a "Rising Star" by *Chambers USA* and *New York Super Lawyers*, and was recognised in *The Legal 500 United States*.



Bridget Treacy, Partner in the London office of Hunton & Williams
+44 (0)20 7220 5731; btreacy@hunton.com

Bridget heads the firm's UK Privacy and Cybersecurity practice and has more than 14 years of extensive experience in privacy law. Her practice focuses on all aspects of privacy, data protection and information governance, particularly for multinational companies. She was ranked by *Computerworld* magazine as one of the top 10 privacy lawyers globally and is ranked as a "Star Individual," the highest honour, by Chambers and Partners.



Rosemary Jay, Consultant Attorney in the London office of Hunton & Williams
+44 (0)20 7220 5753; rjay@hunton.com

Rosemary has practised in privacy law for over 25 years and is recognised as one of the top lawyers in the area of data protection in the UK, with Chambers and Partners recognising her as a "Star Individual," the highest honour. Rosemary is the author of Sweet & Maxwell's *Data Protection Law & Practice*, a contributing editor to *The White Book* on privacy and an editor of the *Encyclopedia of Data Protection and Privacy*.

Our EU Team



David Dumont, Counsel in the Brussels office of Hunton & Williams

+32 (0)2 643 58 18; ddumont@hunton.com

David assists a broad range of clients with all aspects of Belgian and EU data protection law, including HR and customer data privacy issues, implementation of cross-border data transfer strategies and completing registrations with national data protection authorities.



Claire François, Counsel in the Brussels office of Hunton & Williams

+32 (0)2 643 58 04; cfrancois@hunton.com

Claire's practice focuses on EU data protection law with an emphasis on French law. She advises clients on a variety of French and international data compliance projects, including implementation of global data management strategies and international data transfers. Claire also represents clients before the French Data Protection Authority.



James Henderson, Associate in the London office of Hunton & Williams

+44 (0)20 7220 5704; jhenderson@hunton.com

James advises a broad range of clients on all areas of UK and EU data protection law, from general compliance issues and cross-border data transfers to cutting-edge technology issues, such as social media, online behavioural advertising, geolocation and other technology, media and telecommunications matters.

Our EU Team



Laura Leonard, Associate in the Brussels office of Hunton & Williams
+32 (0)2 643 58 30; lleonard@hunton.com

Laura's practice focuses on EU data protection and privacy law. She advises multinational clients on a range of EU data protection and privacy issues, including employee privacy issues, pharmaceutical and medical privacy, international data transfer strategies and other data protection compliance issues.



Anna Pateraki, Associate in the Brussels office of Hunton & Williams
+32 (0)2 643 58 40; apateraki@hunton.com

Anna's practice focuses on all aspects of Global and European data protection law, including global compliance programs, data transfers, data breaches, Privacy Impact Assessments and data processing agreements. She also has experience advising on the EU GDPR and German-related data protection issues.



Julia Senior-Soule, Associate in the London office of Hunton & Williams
+44 (0)20 7220 5607; jseniorsoule@hunton.com

Julia advises clients on all areas of EU data protection law, including the EU General Data Protection Regulation, electronic commerce, analysis of processed data and general compliance issues.



Adam Smith, Associate in the London office of Hunton & Williams
+44 (0)20 7220 5610; asmith@hunton.com

Adam advises clients on all areas of UK and EU data protection law, including cross-border data transfer mechanisms, subject access requests, data breach response, bank secrecy and general privacy compliance issues.

The Centre for Information Policy Leadership



Bojana Bellamy, *President, CIPL*

+44 (0)20 7220 5703; bbellamy@hunton.com

Bojana brings more than 20 years of experience and a deep knowledge of global data privacy and cybersecurity law and policy. She was a board member of the International Association of Privacy Professionals from 2008-2013, and was elected chair from 2011-2012. Bojana was elected to participate in a new transatlantic initiative, the "Privacy Bridge Project", that seeks to develop practical solutions to bridge the gap between the EU and US privacy regimes.



Markus Heyder, *Vice President and Senior Policy Counselor, CIPL*

+1 (202) 419 2005; mheyder@hunton.com

Markus has extensive experience in global data privacy and information security law and policy, including representing the Federal Trade Commission in developing the APEC Cross-Border Privacy Rules helping to create and manage the Global Privacy Enforcement Network, and working on matters relating to the US-EU Safe Harbor Framework. Prior to joining Hunton & Williams, Markus served for over 10 years as Counsel for International Consumer Protection in the Office of International Affairs at the FTC and nearly two years in the FTC's Division of Marketing Practices.



Fred H. Cate, *Senior Policy Advisor, CIPL*

+1 (812) 855 1161; fcate@hunton.com

A distinguished professor and director of the Center for Applied Cybersecurity Research at Indiana University, Professor Cate is a leading authority on privacy, security and other information law and policy issues. He is actively engaged in advising government and industry leaders. He leads the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information.



Richard Thomas, *CBE LLD, Global Strategy Advisor, CIPL*

+44 (0)20 7220 5601; rthomas@hunton.com

Richard has nearly 40 years of experience working across the private and public sectors. He was the Information Commissioner for the UK from November 2002 until his retirement at the end of June 2009. In 2008, he was awarded "Privacy Leader of the Year" by the IAPP and was voted third in Silicon.com's global "IT Agenda Setters" poll.



Samuel Grogan, *Global Privacy Policy Analyst, CIPL*

+1 (202) 778 2211; sgrogan@hunton.com

Sam has extensive experience in global privacy research, including previous work on global data issues at the Stanford Center for Internet and Society and the University of Pennsylvania's Center for Technology, Competition and Innovation. Sam has two LL.M. degrees, one in EU privacy from Queen Mary, University of London, and another from the University of Pennsylvania Law school with a focus on US privacy.



HUNTON &
WILLIAMS

EUregulation@hunton.com