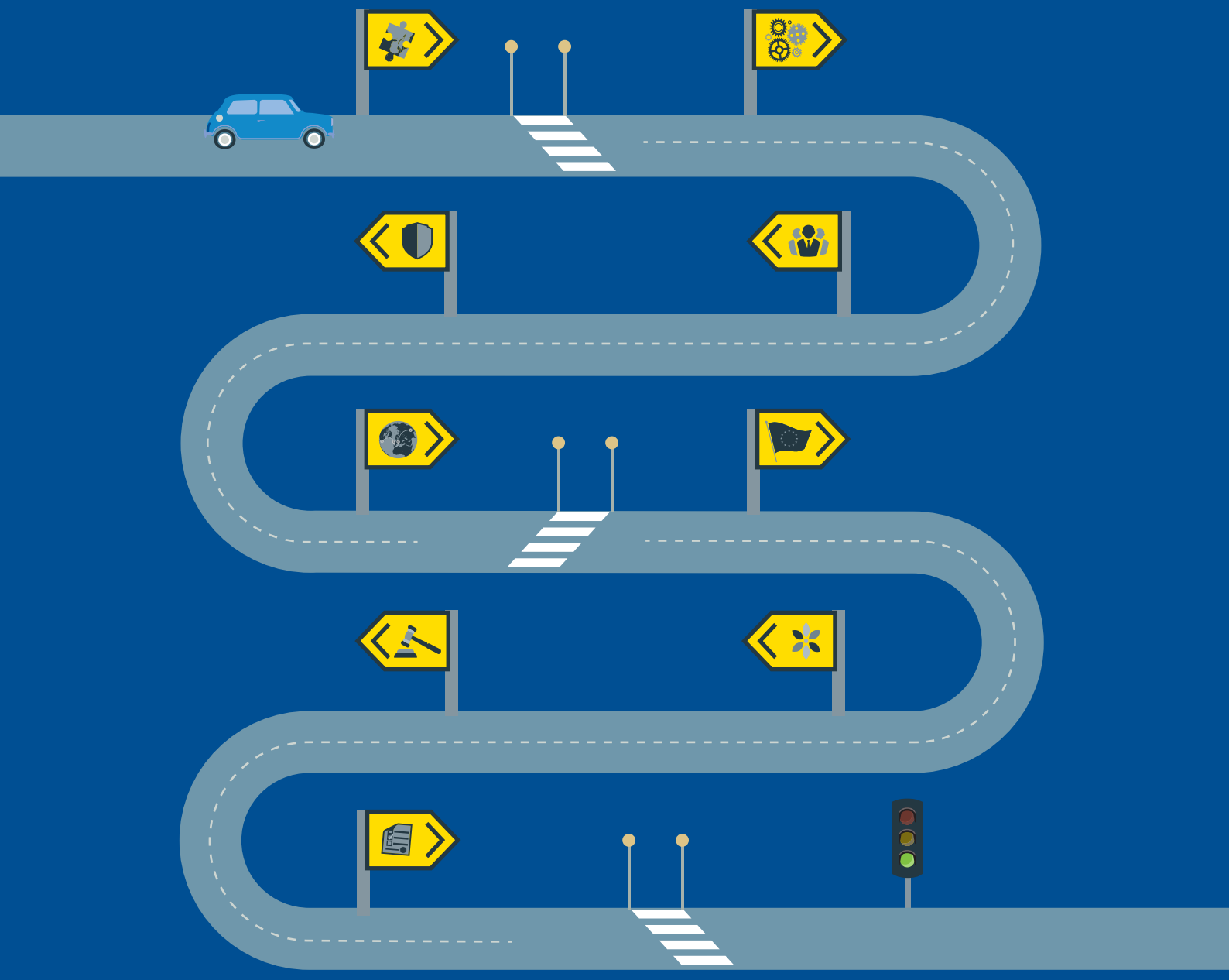
Bird & Bird & guide to the General Data Protection Regulation

April 2016



In publishing a draft General Data Protection Regulation in January 2012, the European Commission fired the starting pistol on 4 years of debate, negotiation and lobbying the like of which the European Union (EU) has never previously seen. This guide summarises the resulting Regulation which emerged from that process – a law which will significantly overhaul Europe's cornerstone data protection legislation at a time when information systems and digital business underpin human life.

The changes which are to be ushered in by the GDPR in 2018 are substantial and ambitious. At over 200 pages long the Regulation is one of the most wide ranging pieces of legislation passed by the EU in recent years, and concepts to be introduced such as the 'right to be forgotten', data portability, data breach notification and accountability (to call out only a few) will take some getting used to. Even its legal medium - a regulation not a directive - makes the GDPR an unusual piece of legislation for data protection lawyers to analyse.

This guide seeks to summarise the key changes that the new law will bring and to highlight the most important actions which organisations should take in preparing to comply with it.

We have divided our summary into chapters which broadly follow those used by the Regulation, but with each sub-divided into themes. Each sub-chapter starts with a speed read summary, a list of suggested priority action points and our assessment of the degree of change which the analysed section of the GDPR will bring (in the form of a pressure dial – ranging from green, indicating a small change, to red, indicating a significant change). We have also included a signpost in each sub-chapter to guide you to where you can find relevant source material within the Regulation.

European data protection law has always been written using a certain amount of jargon and bespoke definitions, and the GDPR is no different. To help those new to this language we have also included a glossary of terms.

This version of the Guide incorporates changes to the Regulation made in the text voted on by European Parliament on 14 April 2016.

As further guidance on the GDPR and implementing provisions emerge from law makers, regulators and the courts, we will continue to publish updates and our own guidance. If you would like to receive details, please let us know. In the meantime, we hope that you will find this guide useful.

Ruth Boardman
Partner, UK

James Mullock
Partner, UK

Ariane Mole
Partner, FR

Table of contents

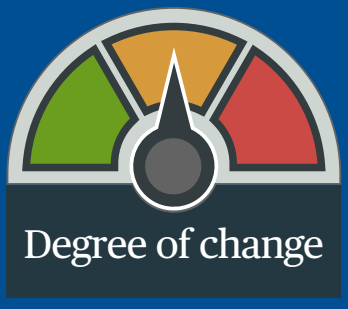
Material and territorial scope

At a glance

- As compared to Directive 95/46/EC (the "Data Protection Directive") which it replaces, the GDPR seeks to extend the reach of EU data protection law.
  - An EU based data controller and processor falls into its scope - where personal data is processed *"in the context of its activities"* a broadly interpreted test.
  - Where no EU presence exists, the GDPR will still apply whenever: (1) an EU resident's personal data is processed in connection with goods/services offered to him/her; or (2) the behaviour of individuals within the EU is *"monitored"*.
- Despite being a Regulation, the GDPR allows Member States to legislate in many areas. This will challenge the GDPR's aim of consistency.
- At the time of going to press we know what the substantive provisions of the GDPR will say (they were finalised in December 2015), but we do not know the precise date in 2018 when they will take effect (the 2 year clock starts after the GDPR's final adoption by EU institutions – expected in Q2 2016).
- The GDPR does not apply to certain activities – including processing covered by the Law Enforcement Agencies ("LEA") Directive, for national security purposes and processing carried out by individuals purely for personal/ household activities.

To do list

- Organisations without an EU presence, but who target EU individuals, should:
  - understand the impact of the GDPR; and
  - determine an approach to compliance.
- Organisations working in areas where *"special"/sectoral* rules are common, should:
  - assess if they require specific Member State laws and advocate these if necessary; and
  - keep a watching brief on such laws being promulgated in ways which may be unhelpful for them.



Territorial scope

EU "established" controllers or processors

The GDPR will apply to organisations which have EU *"establishments"*, where personal data are processed *"in the context of the activities"* of such an establishment.

If this test is met, the GDPR applies irrespective of whether the actual data processing takes place in the EU or not.

"Establishment" was considered by the Court of Justice of the European Union ("CJEU") in the 2015 case of *Weltimmo v NAIH* (C-230/14). This confirmed that establishment is a *"broad"* and *"flexible"* phrase that should not hinge on legal form. An organisation may be *"established"* where it exercises *"any real and effective activity – even a minimal one"* – through *"stable arrangements"* in the EU. The presence of a single representative may be sufficient. In that case, Weltimmo was considered to be established in Hungary as a result of the use of a website in Hungarian which advertised Hungarian properties (which meant that, as a consequence, it was considered *"mainly or entirely directed at that Member State"*), use of a local agent (who was responsible for local debt collection and acted as a representative in administrative and judicial proceedings), and use of a Hungarian postal address and bank account for business purposes – notwithstanding that Weltimmo was incorporated in Slovakia.

Organisations which have EU sales offices, which promote or sell advertising or marketing targeting EU residents will likely be subject to the GDPR – since the associated processing of personal data is considered to be *"inextricably linked"* to and thus carried out *"in the context of the activities of"* those EU establishments *(Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (C-131/12)).

Non-EU "established" organisations who target or monitor EU data subjects

Non-EU established organisations will be subject to the GDPR where they process personal data about EU data subjects in connection with:

- the *"offering of goods or services"* (payment is not required); or
- *"monitoring"* their behaviour within the EU.

Mere accessibility of a site from within the EU is not sufficient. It must be apparent that the organisation *"envisages"* that activities will be directed to EU data subjects.

Contact addresses accessible from the EU and the use of a language used in the controller's own country are also not sufficient. However, the use of an EU language/currency, the ability to place orders in that other language and references to EU users or customers will be relevant.

The CJEU has examined when an activity (such as offering goods and services) will be considered *"directed to"* EU Member States in a separate context (i.e. under the "Brussels 1" Regulation (44/2001/EC) governing *"jurisdiction…in civil and commercial matters"*). Its comments are likely to aid interpretation under this similar aspect of the GDPR. In addition to the considerations mentioned above, the CJEU notes that an intention to target EU customers may be illustrated by: (1) *"patent"* evidence, such as the payment of money to a search engine to facilitate access by those within a Member State or where targeted Member States are designated by name; and (2) other factors – possibly in combination with each other – including the *"international nature"* of the relevant activity (e.g. certain tourist activities), mentions of telephone numbers with an international code, use of a top-level domain name other than that of the state in which the trader is established (such as .de or .eu), the description of *"itineraries…from Member States to the place where the service is provided"* and mentions of an *"international clientele composed of customers domiciled in various Member States"*. This list is *not exhaustive* and the question should be determined on a case-by-case basis *(Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller* (Joined cases (C-585/08) and (C-144/09)).

"Monitoring" specifically includes the tracking of individuals online to create profiles, including where this is used to take decisions to analyse/predict personal preferences, behaviours and attitudes.

Organisations subject to the GDPR's *long-arm* jurisdictional reach must appoint an EU-based representative.

Under the Data Protection Directive, organisations targeting EU data subjects only had to comply with EU rules if they also made use of *"equipment"* in the EU to process personal data. This led national supervisory authorities, who were seeking to assert jurisdiction, to develop arguments that the placing of cookies, or requesting users to fill in forms, would amount to the use of *"equipment"* in the EU. It will now be easier to demonstrate that EU law applies. (Although, where organisations have no EU presence, enforcement may be just as difficult as before).

Where EU member state law applies by virtue of public international law

Recital 26 gives the example of a diplomatic mission or consular position.

Exclusions

Certain activities fall entirely outside the GDPR's scope (listed below).

In addition, the GDPR acknowledges that data protection rights are not absolute and must be balanced (proportionately) with other rights – including the *"freedom to conduct a business"*. (For the ability of Member States to introduce exemptions, see section on derogations and special conditions). As the GDPR toughens up many areas of data protection, introducing more new sticks than regulatory carrots, businesses may find it helpful to bookmark this statement in Recital 4 in case of future need.

The GDPR does not apply to the processing of personal data (these general exemptions are very similar to the equivalent provisions included in the Data Protection Directive):

- in respect of activities which fall outside the scope of EU law (e.g. activities concerning national security);
- in relation to the EU's common foreign and security policy;
- by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences and associated matters (i.e. where the Law Enforcement Agencies ("LEA") Directive[1], initially based on COM(2012) 10 and which was subject to political agreement on 15th December 2015 alongside the GDPR, now applies);
- by EU institutions, where Regulation 45/2001/EC will continue to apply instead of the GDPR. This Regulation is to be updated to ensure consistency with the GDPR; and
- by a natural person as part of a *"purely personal or household activity"*. This covers correspondence and the holding of address books – but it also now covers social networking and online activities undertaken for social and domestic purposes. It represents a possible widening of the exemption from the principles set out in *Bodil Lindqvist* (C-101/01), before the advent of social media. In this case, the CJEU noted that sharing data with the Internet at large *"so that those data are made accessible to an indefinite number of people"* could not fall within this exemption, which it stated should be limited to activities *"carried out in the course of the private or family life of individuals"*. Note also that the GDPR will remain applicable to controllers and processors who *"provide the means for processing"* which falls within this exemption.

The GDPR is stated to be *"without prejudice"* to the rules in the E-commerce Directive (2000/31/EC), in particular to those concerning the liability of *"intermediary service providers"* (and which purport to limit their exposure to pecuniary and criminal liability where they merely host, cache or act as a *"mere conduit"*). The relationship with the E-commerce Directive is not straightforward – as that Directive states that issues relating to the processing of personal data are excluded from its scope and *"solely governed"* by relevant data protection legislation. The two can be read consistently if one assumes that the liability of ISPs for the actions of users will be determined by the E-commerce Directive, but that other matters (such as obligations to erase or rectify data, or obligations on an ISP concerning its own uses of personal data) will be governed by the GDPR. However, the point is not clear.

Regulation versus national law

As a Regulation, the GDPR will be directly effective in Member States without the need for implementing legislation.

However, on numerous occasions, the GDPR does allow Member States to legislate on data protection matters. This includes occasions where the processing of personal data is required to comply with a legal obligation, relates to a public interest task or is carried out by a body with official authority. Numerous articles also state that their provisions may be further specified or restricted by Member State law.

Organisations working in sectors where *special rules* often apply (e.g. health and financial services) should: (1) consider if they would benefit from such *"special rules"* which would particularise or liberalise the GDPR; and (2) advocate these accordingly. They should also watch for Member States seeking to introduce *"special rules"* which may prove restrictive or inconsistent across Member States.

Where can I find this?

Material Scope	*Article 2*	*Recitals 3a and 6-17.*
Territorial Scope	*Article 3*	*Recitals 19-22*

[1] Full title: Directive *"on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data."*

New and significantly changed concepts

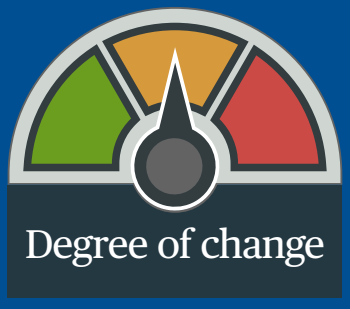
At a glance

The GDPR will introduce significant changes, including via the following concepts:

- *Transparency and Consent* – i.e. the information to be provided to and permissions required from individuals to justify use of their personal data. The GDPR's requirements, including for consent to be unambiguous and not to be assumed from inaction, will mean that many data protection notices will need to be amended.
- *Children and consent* – online, parental prior consent required for use of an under 13 year old's personal data. Member States are free to set their own rules for those aged 13-15 (inclusive). If they choose not to, parental consent is required for children under 16.
- *Regulated data* – the definitions of "Personal Data" and "Sensitive Data" have been expanded, for instance, the latter now includes genetic and biometric data.
- *Pseudonymisation* – a privacy enhancing technique where information which allows data to be attributed to a specific person is held separately and subject to technical and organisational measures to ensure non-attribution.
- *Personal Data Breach* – a new security breach communication law is introduced for all data controllers regardless of their sector.
- *Data protection by design and accountability* – organisations are required to adopt significant new technical and organisational measures to demonstrate their GDPR compliance.
- *Enhanced rights* – Data Subjects are given substantial rights including the right to be forgotten, data portability rights and the right to object to automated decision making.
- *Supervisory authorities and the EDPB* – regulator oversight of data protection will change significantly, including via the introduction of a new single point of reference for multi-national groups.

To do list

No action is required



The GDPR's provisions and the obligations which they bring are extensive, but the following stand out as material new, or varied, concepts. More detailed information on each appears elsewhere in this guide.

Consent

The conditions for obtaining consent have become stricter:

- the data subject must have the right to withdraw consent at any time; and
- separate consents are required for different processing activities and there is a presumption that forced, or 'omnibus', consent mechanisms will not be valid. Further guidance is expected but organisations will need to review existing consent mechanisms, to ensure they present genuine and granular choice.

Consent is not the only mechanism for justifying the processing of personal data. Concepts such as contractual necessity, compliance with a (Member State or EU) legal obligation or processing necessary for legitimate interests remain available.

For more information on this topic, see sections on consent; children; and sensitive data and lawful processing (under the chapter on principles).

Transparency

Organisations will need to provide extensive information to individuals about the processing of their personal data.

The GDPR combines the various transparency obligations which apply across the EU. The list of information to be provided runs to 6 pages in the GDPR, yet data controllers have to achieve what EU law makers have failed to do and must provide information in a concise, transparent, intelligible and easily accessible way.

The use of standardised icons is mooted in the GDPR and the Commission is given the option to choose to introduce these via delegated acts at a later stage.

For more information on this topic, see section on information notices.

Children

Children under the age of 13 can never, themselves, give consent to the processing of their personal data in relation to online services.

For children between the ages of 13 and 15 (inclusive), the general rule is that if an organisation seeks consent to process their personal data, then parental consent must be obtained, unless the relevant individual Member State legislates to reduce the age threshold – although the threshold can never drop below 13 years of age.

Children aged 16 or older may give consent for the processing of their personal data themselves.

There are no specific rules relating to parental consent for offline data processing: usual Member State rules on capacity would apply here.

For more information on this topic, see section on children.

Personal data/ sensitive data ("special categories of data")

The GDPR applies to data from which a living individual is identified or identifiable (by anyone), whether directly or indirectly. The Directive's test of *'all means reasonably likely to be used'* to identify is retained.

The GDPR's recitals highlight that certain categories of online data may be personal – online identifiers, device identifiers, cookie IDs and IP addresses are referenced. Further regulatory and judicial guidance is expected, for instance the CJEU is expected to provide clarification in relation to the status of IP addresses following a referral from the German Supreme Court (Bundesgerichtshof).

"*Special categories of data"* (often referred to as sensitive data) are retained and extended – to cover genetic data and biometric data. As with the current Data Protection Directive, processing of such data is subject to more stringent conditions than other forms of personal data.

Where can I find this?

Definitions *Article 4* *Various (predominantly 24-32)*

Pseudonymisation

A new definition, which refers to the technique of processing personal data in such a way that it can no longer be attributed to a specific *"data subject"* without the use of additional information, which must be kept separately and be subject to technical and organisational measures to ensure non-attribution.

Pseudonymised information is still a form of personal data, but the use of pseudonymisation is encouraged, for instance:

- it is a factor to be considered when determining if processing is *"incompatible"* with the purposes for which the personal data was originally collected and processed;
- it is included as an example of a technique which may satisfy requirements to implement *"privacy by design and by default"* (see section on data governance obligations);
- it may contribute to meeting the GDPR's data security obligations (see section on personal data breaches and notification); and
- for organisations wishing to use personal data for historical or scientific research or for statistical purposes, use of pseudonymous data is emphasised.

Personal data breach communication

The GDPR introduces a security breach communication framework for all data controllers regardless of the sector in which they operate.

Notification obligations (to supervisory authorities and to data subjects) are potentially triggered by *"accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".* For more information on this topic, see section on personal data breaches and notification.

Data protection by design/accountability

Organisations must be able to demonstrate their compliance with the GDPR's principles, including by adopting certain *"data protection by design"* measures (e.g. the use of pseudonymisation techniques), staff training programmes and undertaking audits.

Where "high risk" processing will take place (such as monitoring activities, systematic evaluations or processing special categories of data), a detailed privacy impact assessment ("PIA") must be undertaken and documented. Where a PIA results in the conclusion that there is indeed a high, and unmitigated, risk for the data subjects, controllers must notify the supervisory authority and obtain its view on the adequacy of the measures proposed by the PIA to reduce the risks of processing.

Controllers and processors may decide to appoint a Data Protection Officer ("DPO"). This is obligatory for public sector bodies or those involved in certain listed sensitive activities. Group companies can jointly appoint a DPO.

For more information on these topics see section on data governance obligations.

Enhanced rights for individuals

The GDPR enshrines a wide range of existing and new rights for individuals in respect of their personal data.

These include the right to be forgotten, the right to request the porting of one's personal data to a new service provider, the right to object to certain processing activities and also to decisions taken by automated processes.

For more information on these topics see section on information notices.

Supervisory authorities and the EDPB

Data protection regulators are referred to as supervisory authorities.

A single lead supervisory authority located in the Member State in which an organisation has its "main" establishment will regulate that organisation's compliance with the GDPR.

A European Data Protection Board (EDPB) will be created to (amongst many other things) issue opinions on particular issues and adjudicate on disputes arising from supervisory authority decisions.

For more information on this topic see section on appointment of supervisory authorities.

Data protection principles

At a glance

- The data protection principles are revised but are broadly similar to the principles set out in Directive 95/46/EC (the "Data Protection Directive"): fairness, lawfulness and transparency; purpose limitation; data minimisation; data quality; security, integrity and confidentiality.
- A new accountability principle makes controllers responsible for demonstrating compliance with the data protection principles.

To do list

- ☐ Review data protection policies, codes of conduct and training to ensure these are consistent with the revised principles.
- ☐ Identify means to *"demonstrate compliance"* – e.g. adherence to approved codes of conduct, "paper trails" of decisions relating to data processing and, where appropriate, privacy impact assessments.

Commentary

The principles under the GDPR are broadly similar to those in the Data Protection Directive, but there are some new elements highlighted in italics below.

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly, and *in a transparent manner in relation to the data subject.*

Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of personal data for *archiving purposes in the public interest*, or scientific and historical research purposes or statistical purposes shall not be considered incompatible with the original processing purposes. However, conditions in Article 83(1) (which sets out safeguards and derogations in relation to processing for such purposes) must be met.

Data minimisation

Personal data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed.

Accuracy

Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage limitation

Personal data must be kept *in a form which permits identification of data subjects* for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the data will be processed solely for *archiving purposes in the public interest*, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) and subject to implementation of appropriate technical and organisational measures.

Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

The controller shall be responsible for and be *able to demonstrate* compliance with these principles.

Where can I find this?

Article 5 and Recital 39

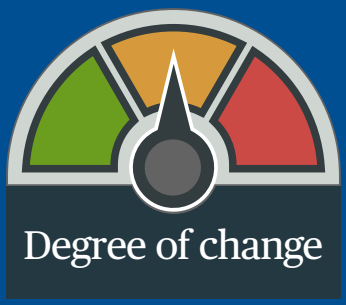
Lawfulness of processing and further processing

At a glance

- The grounds for processing personal data under the GDPR broadly replicate those under the Data Protection Directive.
- There are new limitations on the use of consent and the processing of children's data.
- There are specific restrictions on the ability to rely on "legitimate interests" as a basis for processing and some clarification as to when it may be used.
- There is a non-exhaustive list of factors to be taken into account when determining whether the processing of data for a new purpose is incompatible with the purposes for which the data were initially collected.

To do list

- ☐ Ensure you are clear about the grounds for lawful processing relied on by your organisation and check these grounds will still be applicable under the GDPR.
- ☐ Where relying on consent, ensure quality of consent meets new requirements (see section on consent for further details).
- ☐ Consider whether new rules on children's data are likely to affect you, and, if so, which national rules you will need to follow (see section on children for further details).
- ☐ Ensure that your internal governance processes will enable you to demonstrate how decisions to use data for further processing purposes have been reached and that relevant factors have been considered.



Commentary

Article 6(1) GDPR sets out the conditions that must be satisfied for the processing of personal data to be lawful (For provisions relating to sensitive data see section on sensitive data and lawful processing). These grounds broadly replicate those in the Data Protection Directive. These are:

6(1)(a) - Consent of the data subject

The GDPR approaches consent more restrictively; in particular it seeks to ensure that consent is specific to distinct purposes of processing (see section on consent). Particular conditions are imposed in the case of children (See section on children).

6(1)(b) - Necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract

No change to the position under the Data Protection Directive.

6(1)(c) - Necessary for compliance with a legal obligation

This replicates an equivalent ground under the Data Protection Directive. However, Article 6(3) and Recitals 41 and 45 make it clear that the legal obligation in question must be:

- an obligation of Member State or EU law to which the controller is subject; and
- *"clear and precise"* and its application foreseeable for those subject to it.

The recitals make it clear that the relevant "legal obligation" need not be statutory (i.e. common law would be sufficient, if this meets the *"clear and precise"* test). A legal obligation could cover several processing operations carried out by the controller so that it may not be necessary to identify a specific legal obligation for each individual processing activity.

6(1)(d) - Necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent

Recital 46 suggests that this ground may apply to processing that is necessary for humanitarian purposes (e.g. monitoring epidemics) or in connection with humanitarian emergencies (e.g. disaster response). The recital indicates that in cases where personal data are processed in the vital interests of a person other than the data subject, this ground for processing should be relied on only where no other legal basis is available.

6(1)(e) - Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Article 6(3) and Recital 45 make clear this ground will apply only where the task carried out, or the authority of the controller, is laid down in Union law or Member State law to which the controller is subject.

6(1)(f) - Necessary for the purposes of legitimate interests

This ground can no longer be relied on by public authorities processing personal data in the exercise of their functions; Recitals 47-50 add more detail on what may be considered a *"legitimate interest"*. (See section on legitimate interests for further details).

Member States are permitted to introduce specific provisions to provide a basis under Articles 6(1)(c) and 6(1)(e) (processing due to a legal obligation or performance of a task in the public interest or in the exercise of official authority) for other specific processing situations (e.g. journalism and research). This is likely to result in a degree of variation across the EU. (For further details see section on derogations and special conditions).

Further processing

The GDPR also sets out the rules (at Article 6(4)) on factors a controller must take into account to assess whether a new processing purpose is compatible with the purpose for which the data were initially collected. Where such processing is not based on consent, or on Union or Member State law relating to matters specified in Article 23 (general article on restrictions relating to the protection of national security, criminal investigations etc.), the following factors should be taken into account in order to determine compatibility:

- any link between the original and proposed new purposes;
- the context in which data have been collected (in particular the relationship between subjects and the controller);
- the nature of the data (particularly whether they are sensitive data or criminal data);
- the possible consequences of the proposed processing; and
- the existence of safeguards (including encryption or pseudonymisation).

Recital 50 indicates that further processing for archiving purposes in the public interest, for scientific and historical research purposes or for statistical purposes should be considered as compatible processing (see section on derogations and special conditions).

Where can I find this?

Lawful basis for processing (personal data)
Articles 6-10 Recitals 40 - 50

« Back to Table of Contents

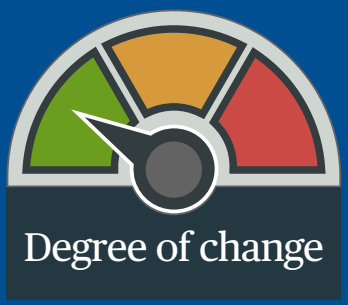
Legitimate interests

At a glance

- Other than in the case of public authorities, *"legitimate interests"*, as a basis for lawful processing, is not substantially changed by the GDPR.
- Public authorities will be unable to rely on *"legitimate interests"* to legitimise data processing carried out in the discharge of their functions.
- Controllers that rely on *"legitimate interests"* should maintain a record of the assessment they have made, so that they can demonstrate that they have given proper consideration to the rights and freedoms of data subjects.

To do list

- ☐ Ensure you are clear about the grounds for lawful processing relied on by your organisation and check these grounds will still be applicable under the GDPR (see section on lawfulness of processing and further processing).
- ☐ If your organisation is a public authority that currently relies on *"legitimate interests"* when processing personal data in connection with the discharge of its functions, seek to identify another legal basis for the processing of this data (e.g. processing necessary in the public interest or in the exercise of official authority).
- ☐ Where relying on *"legitimate interests"*, ensure that decision-making in relation to the balance between the interests of the controller (or relevant third party) and the rights of data subjects is documented, particularly where this affects children. Ensure also that data subjects would reasonably expect their data to be processed on the basis of the legitimate interests of the controller or relevant third party.
- ☐ Where *"legitimate interests"* are relied on, ensure this is included in the information that must be supplied to data subjects pursuant to Articles 13 and 14. (See section on information notices).



Commentary

Article 6(1) of the GDPR states that data processing shall be lawful only where at least one of the provisions at Article 6(1)(a)-(f) applies.

Article 6(1)(f) applies where:

"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

Article 6(1) makes clear that subsection (f) shall not apply to *"processing carried out by public authorities in the performance of their tasks."*

This broadly reproduces an equivalent provision in the Data Protection Directive, except that:

- the need to specifically consider the interests and rights of children is new (see section on children). In practice, this insertion is likely to require controllers to ensure that any decision to process data relating to children on the basis of "legitimate interests" is carefully documented and a risk assessment conducted; and
- *"legitimate interests"* can no longer be relied upon by public authorities in relation to data processed by them when discharging their functions.

What are legitimate interests?

The recitals give examples of processing that could be necessary for the legitimate interest of a data controller. These include:

- Recital 47: processing for direct marketing purposes or preventing fraud;
- Recital 48: transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data (note international transfer requirements will still apply – (see section on transfers of personal data;
- Recital 49: processing for the purposes of ensuring network and information security, including preventing unauthorised access to electronic communications networks and stopping damage to computer and electronic communication systems; and
- Recital 50: reporting possible criminal acts or threats to public security to a competent authority.

Recital 47 also states that controllers should consider the expectations of data subjects when assessing whether their legitimate interests are outweighed by the interests of data subjects. The interests and fundamental rights of data subjects *"could in particular override"* that of the controller where data subjects *"do not reasonably expect further processing."*

Information notices must now set out legitimate interests

Where *"legitimate interests"* are relied on in relation to specific processing operations, this will now need to be set out in relevant information notices, by virtue of Article 13 (1)(d) and 14 (2)(b).

Watch out for Codes of Conduct

Article 40 requires Member States, supervisory authorities, the European Data Protection Board and the Commission to encourage the creation of codes of conduct in relation to a wide range of subjects including the legitimate interests pursued by data controllers in specific contexts. Members of trade associations or similar sector specific bodies should watch for the creation of such codes, which might impose particular additional requirements.

Data transfers - a new ground, but unlikely to ever be of use in practice.

A final outing for legitimate interests comes in Article 49(1), which states that transfers can be made based on *"compelling legitimate interests"* where they are not repetitive, relate to only a limited number of data subjects and where the controller has assessed and ensured adequacy. However, this ground can only be used where the controller cannot rely on any other method of ensuring adequacy, including model clauses, BCRs, approved contracts and all derogations from Article 49(1)(a)-(f).The controller would then need to notify the supervisory authority that it was relying on this ground for transfer. It seems unlikely that an organisation will be able to demonstrate that it was unable to rely on any other grounds for transfer. (See section on transfers of personal data for more information).

Where can I find this?

Legitimate Interests
Articles 6(1)(f), 13(1)(d), 14(2)(b) and 44(1)(h)
Recitals 47, 48, 49, 50

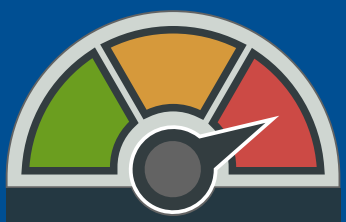
Consent

At a glance

- Consent is subject to additional conditions under the GDPR.
- Additional requirements include an effective prohibition on *"bundled"* consents and the offering of services which are contingent on consent to processing.
- Consent must also now be separable from other written agreements, clearly presented and as easily revoked as given.
- Specific rules will apply to children in relation to information society services.

To do list

- Ensure you are clear about the grounds for lawful processing relied on by your organisation and check these grounds will still be applicable under the GDPR (see section on lawfulness of processing and further processing).
- Consider whether rules on children are likely to affect you, and, if so, which national rules you will need to follow when obtaining consent (see section on children for further details).



Degree of change

To do list (cont.)

- If your organisation relies on consent to process personal data for the purpose of scientific research, consider offering data subjects the opportunity to consent only to certain areas of research or parts of research projects.
- Where relying on consent as the basis for lawful processing, ensure that:
  - consent is active, and does not rely on silence, inactivity or pre-ticked boxes;
  - consent to processing is distinguishable, clear, and is not *"bundled"* with other written agreements or declarations;
  - supply of services is not made contingent on consent to processing which is not necessary for the service being supplied;
  - data subjects are informed that they have the right to withdraw consent at any time but that this will not affect the lawfulness of processing based on consent before its withdrawal;
  - there are simple methods for withdrawing consent, including methods using the same medium used to obtain consent in the first place;
  - separate consents are obtained for distinct processing operations; and
  - consent is not relied on where there is a clear imbalance between the data subject and the controller (especially if the controller is a public authority).

Commentary

Consent - a wider definition

Article 4(11) GDPR defines *"the consent of the data subject"* as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."*

The requirement that consent be *"unambiguous"* does not represent a change for practical purposes; Article 7(a) of Directive 95/46/EC (the "Data Protection Directive") stipulated that where consent is relied on for making data processing legitimate it must be given *"unambiguously"*. Recital 25 suggests that this may be signified by:

"ticking a box when visiting a… website, choosing technical settings… or by any other statement or conduct which clearly indicates… the data subject's acceptance of the proposed processing of their personal data. Silence, pre-ticked boxes or inactivity should therefore not constitute consent."

Explicit consent is still required to justify the processing of sensitive personal data (unless other grounds apply (on which see section on sensitive data and lawful processing).

Steps to validity - distinguishable, revocable and granular

Article 7(1) GDPR requires that where consent is relied on as a ground for lawful processing, controllers should be able to demonstrate that consent was given by the data subject to the processing. The rest of Article 7 is dedicated to setting out the conditions for a valid consent. These are:

- Art 7(2): Consent to processing contained in a written declaration produced by the controller must be distinguishable from other matters in that declaration, intelligible, easily accessible and be in clear and plain language. Recital 42 cites the Unfair Terms in Consumer Contracts Directive (Directive 93/13/EEC) as the inspiration for these obligations. In practice, this will require consent to processing to be clearly distinguishable within broader contracts or agreements.

  Recital 42 also notes that consent will be informed only where the data subject is aware of (at least) the identity of the controller and the intended purposes of processing;

- Art 7(3): Data subjects must have the right to revoke their consent at any time, and it must be as easy to withdraw consent as it is to give it. In practice, as a minimum this is likely to require organisations to allow consent to be withdrawn through the same media (e.g. website, email, text) as it was obtained. The GDPR acknowledges that the withdrawal of consent does not retrospectively render processing unlawful, but requires the controller to inform data subjects of this before consent is given; and

- Art 7(4): Where the performance of a contract, including the provision of a service, is made conditional on consent to the processing of data that is not necessary for the performance of that contract, this is likely to call into question the extent to which consent can be considered to be freely given.

Recital 43 indicates that consent will be presumed not to be freely given if,

- despite it being appropriate in the circumstances, there is no provision for separate consent to be given to different processing operations; or

- *"the performance of a contract, including the provision of a service, is dependent on the consent, despite such consent not being necessary for such performance."*

As a result, the provision of a service should not be made contingent on the data subject's consent to the processing of his/her data for purposes that are unnecessary for the provision of the service.

Children and research

Specific conditions apply to the validity of consent given by children in relation to information society services, with requirements to obtain and verify parental consent below certain age limits (see section on children for further details).

Recital 33 GDPR addresses consent that is obtained for scientific research purposes. It acknowledges that *"it is often not possible to fully identify the purpose of data processing for scientific research purposes at the time of data collection"* and states that:

- data subjects should be able to consent to certain areas of scientific research, where this meets *"recognised ethical standards"* for such research; and

- data subjects should be able to grant consent only to *"certain areas… or parts of research projects to the extent allowed by the intended purpose"*.

Where can I find this?

Articles 4(11), 6(1)(a), 7, 8 and 9(2(a))
Recitals 32, 33, 42 and 43

« Back to Table of Contents

Children

At a glance

- There is a handful of child-specific provisions in the GDPR, particularly in relation to grounds for processing and notices.
- Children are identified as *"vulnerable individuals"* and deserving of *"specific protection"*.
- Processing of data relating to children is noted to carry certain risks, and further restrictions may be imposed as a result of codes of conduct.
- The GDPR does not prescribe the age at which a person is considered to be a child.
- Where online services are provided to a child and consent is relied on as the basis for the lawful processing of his or her data, consent must be given or authorised by a person with parental responsibility for the child. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit -which may be no lower than 13).

To do list

☐	Consider whether rules on children are likely to affect you.
☐	If your organisation offers information society services directly to children, assess which national rules will apply and ensure that appropriate parental consent mechanisms are implemented, including verification processes.
☐	Remain aware of national legislation for offline data processing relating to children's data.
☐	Where services are offered directly to a child, ensure notices are drafted clearly with a child's understanding in mind.
☐	Ensure any reliance on *"legitimate interests"* to justify processing children's data is backed up with a careful and documented consideration of whether a child's interests override those of your organisation.
☐	Be watchful for relevant codes of conduct which might affect any associations or groups your organisation might participate in.

Commentary

The importance of protecting children is mentioned several times in the GDPR. In practice, there is little new harmonisation offered in the final text, and substantive restrictions will likely come either from existing or new national laws or codes of conduct. (See section on codes of conduct and certifications for further details.)

Parental consent

Directive 95/46/EC (the "Data Protection Directive") did not contain any specific restrictions on processing children's data, and rules on children's ability to consent have been drawn from national laws. The GDPR does not offer much harmonisation. The major provision in relation to children is Article 8, which requires parental consent to be obtained for information society services offered directly to a child under the age of 16 – although this ceiling can be set as low as 13 by a Member State, and only applies where the processing would be based on the child's consent.

The controller is also required, under Article 8(2) GDPR, to make *"reasonable efforts"* to verify that consent has been given or authorised by the holder of parental responsibility in light of available technology.

This only affects certain online data – offline data will continue to remain subject to the usual Member State rules on capacity to consent. Article 8(1) is also not to be considered as affecting the general contract law of Member States regarding the validity, formation or effect of a contract with a child. Organisations will still need to consider local laws in this area.

Notices addressed to children must be child-friendly

Article 12 GDPR provides that the obligations to ensure that information provided to data subjects is concise, transparent and in plain language are to be met "in particular for any information addressed specifically to a child". Recital 58 expands:

"Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."

The term *"child"* is not defined by the GDPR. Controllers should therefore be prepared to address these requirements in notices directed at teenagers and young adults.

Miscellaneous provisions - helplines, codes of conduct and work for supervisory authorities

Article 6(1)(f) GDPR notes that the rights and freedoms of a data subject may *"in particular"* override the interests of the controller or third party where the relevant data subject is a child. Controllers should ensure that documentation is kept demonstrating that relevant competing interests have been appropriately considered where relying on legitimate interests for processing data relating to children.

Recital 38 notes that the use of child data in marketing, or for profiling purposes or in connection with the supply of services to children are areas of concern requiring specific protection under the GDPR. The recital also states that parental consent should not be required in the context of preventative and/or counselling services offered directly to a child although this suggestion does not appear to be reflected in the articles of the GDPR itself.

Recital 75 notes that children are *"vulnerable natural persons"* and that processing children's data is an activity that may result in risk *"of varying likelihood and severity"*.

Article 40 requires Member States, supervisory authorities, the European Data Protection Board and the Commission to encourage the creation of codes of conduct, including in the area of the protection of children, and concerning the way in which consent can be collected from the holder of relevant parental responsibility. Organisations that process personal data relating to children should watch for the creation of such codes, which might impose particular additional requirements.

Finally, supervisory authorities, when promoting public awareness and understanding of risks, rules, safeguards and rights in relation to the processing of personal data, pursuant to the obligation imposed on them by Article 57(1)(b), are required to give *"specific attention"* to activities addressed to children.

Where can I find this?

Articles 6(1)(f), 8, 12(1), 40(2)(g), 57(1)(b)
Recitals 38, 58, 75

Sensitive data and lawful processing

At a glance

- "*Special categories of personal data*" (sensitive data) now expressly include *"genetic data"* and *"biometric data"* where processed *"to uniquely identify a person"*.
- The grounds for processing sensitive data under the GDPR broadly replicate those under the Data Protection Directive, although there are wider grounds in the area of health and healthcare management.
- There is also a broad ability for Member States to adduce new conditions (including limitations) regarding the processing of genetic, biometric or health data.

To do list

- ☐ Ensure you are clear about the grounds relied on by your organisation to process sensitive data, and check these grounds will still be applicable under the GDPR;
- ☐ Where relying on consent, ensure the quality of consent meets new requirements in relation to the collection of consent (see section on consent);
- ☐ Consider whether rules on children are likely to affect you, and, if so, which national rules you will need to follow when obtaining their consent (see section on children for further details); and
- ☐ If you process substantial amounts of genetic, biometric or health data, ensure you pay attention to national developments as Member States have a broad right to impose further conditions - including restrictions - on the grounds set out in the GDPR.

Commentary

Article 9(2) sets out the circumstances in which the processing of *sensitive personal data* which is otherwise prohibited, may take place. The following categories of data are considered *"sensitive"*, as set out in Article 9(1):

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- data concerning health or sex life and sexual orientation;
- genetic data (*new*); and
- biometric data where processed to uniquely identify a person (*new*).

Note that Recital 51 suggests that the processing of photographs will not automatically be considered as sensitive processing (as has been the case in some Member States to date); photographs will be covered only to the extent they allow the unique identification or authentication of an individual as a biometric (such as when used as part of an electronic passport).

The grounds for processing sensitive data broadly replicate those in the Data Protection Directive. These are:

9(2)(a) - Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

There is no change here, although new conditions for consent should be considered (see section on consent).

9(2)(b) - Necessary for the carrying out of obligations under employment, social security or social protection law, or a collective agreement

This expands slightly on the wording of the Data Protection Directive by making express reference to compliance with collective agreements and obligations under social security and social protection law.

9(2)(c) - Necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent

This replicates an equivalent provision in the Data Protection Directive.

9(2)(d) - Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

This replicates an equivalent provision in the Data Protection Directive.

9(2)(e) - Data manifestly made public by the data subject

This replicates an equivalent provision in the Data Protection Directive.

9(2)(f) - Necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

The processing of data by courts acting in their judicial capacity is added to the equivalent provision in the Data Protection Directive.

9(2) (g) - Necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures.

This enables Member States to extend by law the circumstances where sensitive data may be processed in the public interest.

9(2)(h) - Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

AND

9(2)(i) - Necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

These two provisions expand the equivalent provision in the Data Protection Directive and address acknowledged gaps in that Directive, by, for example, providing a formal legal justification for regulatory uses of health data in the health and pharmaceutical sectors, and by providing for the sharing of health data with providers of social care

Both conditions require obligations of confidentiality to be in place by way of additional safeguards.

9(2)(j) - necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

This makes new provision for the processing of sensitive personal data for the purposes of archiving, research and statistics, subject to compliance with appropriate safeguards, including safeguards to ensure respect for the principle of data minimisation (see section on derogations and special conditions for further details).

Genetic, biometric, or health data

Member States are entitled, under Article 9(4) GDPR, to maintain or impose further conditions (including limitations) in respect of genetic, biometric or health data. As such, existing differences in approach on these topics will likely be maintained, and further divergence will be permitted. Entities that process these categories of data should continue to keep the development of relevant national law under review and consider the need for further lobbying work in this area.

Criminal convictions and offences

Data relating to criminal convictions and offences are not categorised as *"sensitive"* for the purposes of GDPR. This does not, however, amount to a change as (although the UK Data Protection Act treats personal data relating to criminal proceedings and convictions as sensitive data), data of this kind was not treated as sensitive data under the Data Protection Directive.

The rules under the GDPR in relation to data concerning criminal convictions and offences mirror those which applied under the Data Protection Directive. Article 10 provides that such data may be processed only under the control of official authority or where the processing is authorised by Union law or Member State law that provides appropriate safeguards. This provision is likely to lead to continued national divergence in this area.

Where can I find this?

Article 9 *Recitals 51-56*

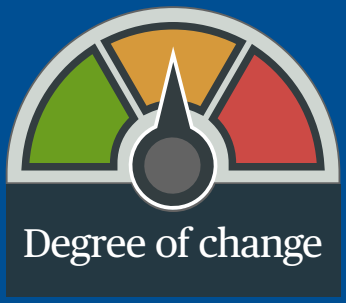
Information notices

At a glance

- Controllers must provide information notices, to ensure transparency of processing.
- Specified information must be provided, and there is also a general transparency obligation.
- Much of the additional information will not be difficult to supply – although it may be hard for organisations to provide retention periods
- There is an emphasis on clear, concise notices.

To do list

- ☐ Audit existing information notices and review and update them.
- ☐ For data which is collected indirectly, ensure that notice is given at the appropriate time.
- ☐ Work with relevant partners who may collect data on your organisation's behalf to assign responsibility for notice review, update and approval.



Commentary

The principle of *"fair and transparent"* processing means that the controller must provide information to individuals about its processing of their data, unless the individual already has this information. The information to be provided is specified in the GDPR and listed below. The controller may also have to provide additional information if, in the specific circumstances and context, this is necessary for the processing to be fair and transparent.

The information must be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language (in particular where the data subject is a child).

What must a controller tell individuals?

The GDPR requires more extensive information to be provided than the Data Protection Directive – although much of the additional information is already mandatory in some Member States.

Information which is not specified in the Data Protection Directive is indicated in italics.

- Identity and contact details of the controller (or its representative, for a non-EU established controller); *contact details of the data protection officer*.
- Purposes of processing *and legal basis for processing – including the "legitimate interest" pursued by the controller (or third party) if this is the legal basis.*
- Recipients, or categories of recipients.
- *Details of data transfers outside the EU:*
  - *including how the data will be protected (e.g. the recipient is in an adequate country; Binding Corporate Rules are in place etc.); and*
  - *how the individual can obtain a copy of the BCRs or other safeguards, or where such safeguards have been made available.*
- *The retention period for the data – if not possible, then the criteria used to set this.*
- That the individual has a right to access *and port data, to* rectify, erase *and restrict his or her personal data, to object to processing and, if processing is based on consent, to withdraw consent*.
- *That the individual can complain to a supervisory authority.*
- *Whether there is a statutory or contractual requirement to provide the data and the consequences of not providing the data.*
- If there will be any automated decision taking – together with information about the logic involved and the significance and consequences of the processing for the individual.

When must a controller provide this information?

Controller obtains information directly from individual

- At the time the data are obtained.

The controller must also tell individuals what information is mandatory and the consequences of not providing information.

Controller does not obtain directly

- Within a reasonable period of having obtained the data (max one month); or
- If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

The controller must also tell individuals the categories of information and the source(s) of the information, including if it came from publicly accessible sources.

- The controller does not have to provide this information to the individual if it would be impossible or involve a disproportionate effort. In these cases, appropriate measures must be taken to protect individuals' interests and the information notice must be made publicly available.

  There is also no need to provide the information notice:

  - if there is an EU or member state law obligation for the controller to obtain/disclose the information; or
  - if the information must remain confidential, because of professional or statutory secrecy obligations, regulated by EU or Member State law.

If the controller later processes personal data for a new purpose, not covered in the initial notice, then it must provide a new notice covering the new processing.

Providing all of this information is hard to reconcile with the GDPR's own requirement of conciseness and clarity. To help better achieve this, there is an ability for the Commission to introduce standardised icons by means of delegated acts. If introduced, these would then also need to be displayed to individuals.

Where can I find this?

Articles 12 and 13
Recitals 58, 60, 61 and 62

Subject access, rectification and portability

At a glance

- Data controllers must, on request:
  - confirm if they process an individual's personal data;
  - provide a copy of the data (in commonly used electronic form in many cases); and
  - provide supporting (and detailed) explanatory materials.
- Data subjects can also demand that their personal data be ported to them or a new provider in machine readable format if the data in question was: 1) provided by the data subject to the controller; 2) is processed automatically; and 3) is processed based on consent or fulfilment of a contract.
- The request must be met within one month (with extensions for some cases) and any intention not to comply must be explained to the individual.
- Access rights are intended to allow individuals to check the lawfulness of processing and the right to a copy should not adversely affect the rights of others.

To do list

☐	Review customer facing team's processes, procedures and training – are they sufficient to deal with the GDPR's access and portability rules?
☐	Develop template response letters, to ensure that all elements of supporting information are provided.
☐	Assess your organisation's ability to provide data in compliance with the GDPR's format obligations. It may be necessary to develop formatting capabilities to meet access requests.
☐	If portability applies, consider if data can easily be exported in structured, machine-readable (and possibly interoperable) formats. Consider if the data relate to more than one data subject and how to address the difficulties this raises.
☐	Consider developing data subject access portals, to allow direct exercise of subject access rights.

Degree of change

Right of information and access

An individual has the following rights with regards to a data controller:

- to obtain confirmation whether his/her personal data are being processed;
- to access the data (i.e. to a copy); and
- to be provided with supplemental information about the processing.

As with all data subject rights, the controller must comply *"without undue delay"* and *"at the latest within one month"*, although there are some possibilities to extend this.

The controller must also use reasonable means to verify the identity of the person making the request – but should not keep or collect data just so as to be able to meet subject access requests. These points are particularly pertinent to online services.

Right of access to data

The controller must provide *"a copy of the personal data undergoing processing"*. This must be provided free of charge (a change for UK based controllers), although the controller may charge a reasonable, administrative-cost fee, if further copies are requested.

If the request is made in electronic form, the information should be provided in a commonly used electronic form (unless the data subject requests otherwise). This could impose costs on controllers who use special formats, or who hold paper records.

Recital 63 also suggests that, where possible, the controller may provide a secure system which would grant the data subject direct access to his/her data. This seems to be encouraged rather than required.

Supplemental information

The controller must also provide the following information (the items in italics are not currently mandated by the Data Protection Directive – although they are required under some Member State laws implementing the Data Protection Directive):

- the purposes of processing;
- the categories of data processed;
- the recipients, or categories of recipients *(in particular, details of disclosure to recipients in third countries or to international organisations* (bodies governed by public international law or set up by agreement between countries));
- *the envisaged retention period, or, if this is not possible, the criteria used to determine this period;*
- *the individual's rights of rectification or erasure, to restrict processing or to object to processing and to lodge a complaint to a supervisory authority;*
- *information regarding the source of the data (if not collected from the data subject);*and
- any regulated automated decision taking (i.e. decisions taken solely on an automated basis and having legal or similar effects; also, automated decision taking involving sensitive data) – including information about the logic involved and the *significance and envisaged consequences of the processing for the data subject.*

If the controller does not intend to comply with the request, he must also provide reasons.

Exemptions

The GDPR recognises that subject access may adversely affect others and provides that the right to receive a copy of the data shall not adversely affect such rights. Recital 63 notes that this could extend to protection of IPR and trade secrets (for example, if release of the logic of automated decision taking would involve release of such information). However, the recital also notes that a controller cannot refuse to provide *all* information, on the basis that access may infringe others' rights.

Recital 63 also contains two other useful limiting provisions:

- if the controller holds a large quantity of data, it may ask the data subject to specify the information or processing activities to which the request relates. (However, the recital does not go on to say that there is any exemption due to large volumes of relevant data: the limitation seems to be more to do with the specificity of the request, rather than the extent of time and effort on the controller's part – although the two may, of course, be linked);
- the data subject's right is *"to be aware of and verify the lawfulness of the processing"*. This confirms the comments made by the CJEU in *YS v Minister voor Immigratie, Integratie en Asiel* (Case C-141/12) that the purpose of subject access requests is to allow the individual to confirm the accuracy of data and confirm the lawfulness of processing and to allow them to exercise rights of correction or objection etc if necessary. In other words, the purpose is related to the individual's rights under data protection legislation: requests made for other, non-data protection purposes, may possibly be rejected.

Rectification

Individuals can require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.

Portability

The subject access right provided under the GDPR already gives individuals the right to require their data to be provided in a commonly used electronic form.

Data portability goes beyond this and requires the controller to provide information in a structured, commonly used and machine readable form. Further, the controller can be required to transmit the data directly to another controller. There is some uncertainty whether the format must be interoperable, or whether this is a matter of best practice which controllers are encouraged to adopt.

Whereas subject access is a broad right, portability is narrower. It applies:

- to personal data which is processed by automated means (no paper records);
- to personal data which the data subject has provided to the controller; and
- only where the basis for processing is consent, or that the data are being processed to fulfil a contract or steps preparatory to a contract.

The data which are being ported may relate to more than one individual: the obligation to port the data is stated to be without prejudice to the rights of other data subjects. Presumably, a controller should not port data to another controller (or to the individual) if this would breach the rights of others. It is not clear how a controller (for example a social media provider) would be expected to make this assessment.

Where can I find this?

Subject access	*Article 15*	*Recitals 59, 63, 64*
Rectification	*Article 16*	*-*
Portability	*Article 20*	*Recital 68*

Rights to object

At a glance

- There are rights for individuals to object to specific types of processing:
  - Direct marketing;
  - Processing based on legitimate interests or performance of a task in the public interest/ exercise of official authority; and
  - Processing for research or statistical purposes.
- Only the right to object to direct marketing is absolute (i.e. no need to demonstrate grounds for objecting, no exemptions which allow processing to continue).
- There are obligations to notify individuals of these rights at an early stage - clearly and separately from other information.
- Online services must offer an automated method of objecting.

To do list

- ☐ Audit data protection notices and policies to ensure that individuals are told about their right to object, clearly and separately, at the point of 'first communication';
- ☐ For online services, ensure there is an automated way for this to be effected; and
- ☐ Review marketing suppression lists and processes (including those operated on behalf of your organisation by partners and service providers) to ensure they are capable of operating in compliance with the GDPR.

Rights to object

Three rights to object are given by the GDPR. All relate to processing carried out for specific purposes, or which is justified on a particular basis. There is no right for an individual to object to processing in general.

The rights are to object to:

Processing which is for direct marketing purposes

This is an absolute right; once the individual objects, the data must not be processed for direct marketing any further.

Processing for scientific/historical research/statistical purposes

Less strong than the right to object to direct marketing – there must be *"grounds relating to[the data subject's] particular situation"*.

There is an exception where the processing is necessary for the performance of a task carried out for reasons of public interest.

There is no equivalent to this provision in the Data Protection Directive.

Processing based on two specific purposes:

Again, this can be exercised on grounds relating to the data subject's particular situation.

1. legitimate interest grounds (i.e. under Art. 6(1)(f)); or
2. because it is necessary for a public interest task/official authority (i.e. Art. 6(1)(e))

Again, this can be exercised on grounds relating to the data subject's particular situation.

The controller must then cease processing of the personal data unless:

- it can demonstrate compelling legitimate grounds which override the interests of the data subject; or
- the processing is for the establishment, exercise or defence of legal claims.

So, once an individual objects, based on his or her specific situation, the burden falls to the controller to establish why it should, nonetheless, be able to process personal data on this basis.

This is a tightening of the rules from the Data Protection Directive. In the equivalent provision, it is the data subject who has to demonstrate 'compelling legitimate grounds' of objection and the processing only has to cease if the objection is justified.

Notify individuals of their rights

In the case of processing for direct marketing and processing based on tasks in the public interest/legitimate interests, the individual's right to object must be explicitly brought to his or her attention – at the latest at the time of first communication with the individual. This must be presented clearly and separately from other information.

This need to inform the individual does not apply to statistical/research based processing.

In the case of online services, the individual must be able to exercise his or her right by automated means.

Where can I find this?

Article 21 *Recitals 69 and 70*

Right to erasure and right to restriction of processing

At a glance

- More extensive, and unclear, rights are introduced: a right to be forgotten (now called erasure) and for processing to be restricted.
- Individuals can require data to be 'erased' when there is a problem with the underlying legality of the processing or where they withdraw consent.
- The individual can require the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved, or if the processing is unlawful but the individual objects to erasure.
- Controllers who have made data public which is then subject to a right to erasure request, are required to notify others who are processing that data with details of the request. This is a new wide-ranging and challenging obligation.

To do list

- ☐ Ensure that members of staff and suppliers who may receive data erasure requests recognise them and know how to deal with them.
- ☐ Determine if you work in a sector where compliance with erasure requirements would be so unreasonable and unwarranted that additional Member State-based exemptions should be sought.
- ☐ Determine if systems are able to meet the requirements to mark data as restricted whilst complaints are resolved: undertake development work if needed.

Degree of change

Right to be forgotten

Individuals have the right to have their data 'erased' in certain specified situations - in essence where the processing fails to satisfy the requirements of the GDPR. The right can be exercised against controllers, who must respond without undue delay (and in any event within one month, although this can be extended in difficult cases).

When does the right apply?

- When data are no longer necessary for the purpose for which they were collected or processed.
- If the individual withdraws consent to processing (and if there is no other justification for processing).
  - There is a further trigger relating to withdrawal of consent previously given by a child in relation to online services. However, this seems to add nothing to the general principle that consent can be revoked and, where this is done, that the individual can require the data to be erased.
- To processing based on legitimate interests - if the individual objects and the controller cannot demonstrate that there are overriding legitimate grounds for the processing.
- When the data are otherwise unlawfully processed (i.e. in some way which is otherwise in breach of the GDPR).
- If the data have to be erased to comply with Union or Member State law which applies to the controller.

The last condition could, for example, apply if an individual considers that a data controller is retaining personal data where legislation stipulates that such data (for example an employment related check) must be deleted after a specified period of time.

The general catch-all allowing erasure requests to be made where data are *'unlawfully'* processed is potentially onerous: there are many reasons why data could be processed unlawfully under the GDPR (they may be inaccurate; an element of an information notice may not have been provided to the individual). However, it is not obvious that this should ground a right for the data to be erased. The equivalent provision the Data Protection Directive left more discretion requiring erasure 'as appropriate'. It will be important to see how Member States draft exemptions.

Data put into the public domain

If the controller has made personal data public, and where it is obliged to erase the data, the controller must also inform other controllers who are processing the data that the data subject has requested erasure of those data. The obligation is intended to strengthen individual's rights in an online environment.

The obligation is to take *reasonable steps* and account must be taken of available technology and the cost of implementation. However, the obligation is potentially wide-reaching and extremely difficult to implement: for example, as this is now public domain data, one question is how the original controller will be able to identify the controllers it needs to notify.

Other obligations to notify recipients

If the controller has to erase personal data, then the controller must notify any one to whom it has disclosed such data, unless this would be impossible or involve disproportionate effort.

Exemptions

The obligation does not apply if processing is necessary:

- for the exercise of the right of freedom of expression and information;
- for compliance with a Union or Member State legal obligation;
- for performance of a public interest task or exercise of official authority;
- for public health reasons;
- for archival, research or statistical purposes (if any relevant conditions for this type of processing are met); or
- if required for the establishment, exercise or defence of legal claims.

See section on derogations and special conditions for other occasions when exemptions may be relevant - if provided for under Union or Member State law.

Right to restriction of processing

This replaces the provisions in the Data Protection Directive on 'blocking'. In some situations, this right gives an individual an alternative to requiring data to be erased; in others, it allows the individual to require data to be held in limbo whilst other challenges are resolved.

What is restriction?

If personal data are 'restricted', then the controller may only store the data. It may not further process the data unless:

- the individual consents; or
- the processing is necessary for establishment etc. of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important (Union or Member State) public interest.

Where the data are processed automatically, then the restriction should be effected by technical means and noted in the controller's IT systems. This could mean moving the data to a separate system; temporarily blocking the data on a website or otherwise making the data unavailable.

If the data have been disclosed to others, then the controller must notify those recipients about the restricted processing (unless this is impossible or involves disproportionate effort).

The controller must notify the individual before lifting a restriction.

When is restriction applicable?

- When an individual disputes data accuracy, then personal data will be restricted for the period during which this is verified;
- When an individual has objected to processing (based on legitimate interests), then the individual can require the data to be restricted whilst the controller verifies the grounds for processing;
- When the processing is unlawful but the individual objects to erasure and requests restriction instead; and
- When the controller has no further need for the data but the individual requires the personal data to establish, exercise, or defend legal claims.

This last condition could, for example, mean that controllers are obliged to retain data storage solutions for former customers if the personal data are relevant to proceedings in which the individual is involved.

Where can I find this?

Right to erasure	*Article 17 and 19*	*Recitals 65, 66, 73*
Right to restriction	*Article 17 and 19*	*Recitals 67 and 73*

Profiling and automated decision-taking

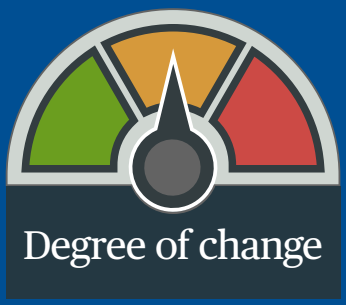
At a glance

- The automated decision-taking rules are similar to the equivalent rules contained in the Data Protection Directive (proposals to introduce restrictions on any 'profiling' were, in the end, not included in the final GDPR).
- The rules affect decisions:
  - taken solely on the basis of automated processing; and
  - which produce legal effects or have similarly significant effects.
- Where the decision is:
  - necessary for the entry into or performance of a contract; or
  - authorised by Union or Member State law applicable to the controller; or
  - based on the individual's explicit consent

  then automated processing can be used. However, suitable measures to protect the individual's interests must still be in place.
- There are additional restrictions on profiling based on sensitive data – which need explicit consent, or to be authorised by Union or Member State law which is necessary for substantial public interest grounds.

To do list

- ☐ Check what significant automated decision-taking is used. Identify any decisions which rely on
  - Consent;
  - Authorisation by law;
  - or which relate to sensitive data or children.
- ☐ If profiling is based on consent, ensure this is explicit.
- ☐ If profiling is authorised by law, check if this is Union or Member State law; maintain a watching brief to see if Member States will seek to make any changes to the law to reflect the GDPR.
- ☐ If profiling is based on sensitive data:
  - Check if you can obtain explicit consent;
  - If not, you will need to lobby for Member State (or Union) legal support for such processing.
- ☐ If profiling involves children, seek advice: this is restricted.



Meaning of profiling

Profiling is *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement"*.

During the legislative process, there were attempts to introduce significant restrictions on all profiling. However, in the end, these were not included – although Recital 72 does note that the EDPB may publish guidance on profiling.

Restrictions on automated decision-taking with significant effects

Restrictions on decisions based solely on automated processing (which could include profiling), apply if the decisions produce legal effects or similarly significantly affects the data subject. Recital 71 gives the example of online credit decisions and e-recruiting; it also makes clear that the objectionable element is the lack of human intervention.

Individuals have a right not to be subject to such decisions. (This could either be read as a prohibition on such processing or that the processing may take place but that individuals have a right to object to it. This ambiguity is also present in the Data Protection Directive and Member States differ in their approaches to the point).

Such significant automated processing can be used if it is:

- necessary to enter into, or to perform, a contract between a data subject and controller;
- authorised by Union or Member State law; or
- based on the individual's explicit consent.

Profiling based on explicit consent or contractual fulfilment

In the first and third cases (contract performance and consent), the controller must implement suitable measures to safeguard the data subject. At a minimum, this must include a right to obtain human intervention for the data subject to be able to express his or her point of view and to contest the decision.

The equivalent provisions in the Data Protection Directive stated that this was not necessary if the effect of the decision was to grant the individual's request. This is not carried across into the GDPR perhaps because in contexts such as finance and insurance, as long as a contract is offered (even if on difficult terms), the controller could say that the individual's request had been granted, thus avoiding the purpose of the provisions.

Recital 71 emphasises that appropriate statistical techniques must be used; that transparency must be ensured; that measures should be in place to correct inaccuracies and risks of errors; and that security must be ensured and discriminatory effects prevented. Recital 71 also notes that such measures should not concern children.

Authorisation by law

In the second case (authorisation by law) the law itself must contain suitable measures to safeguard the individual's interests. Recital 71 mentions profiling to ensure security and reliability of services or in connection with monitoring of fraud and tax evasion as types of automated decisions which could be justified based on Union or Member State law.

Sensitive data

Automated decision-taking based on sensitive data is further restricted. Decisions based on these types of data may only take place:

- with explicit consent; or
- where the processing is necessary for substantial public interest reasons and on the basis of Union or Member State law – which must include measures to protect the interests of the data subjects.

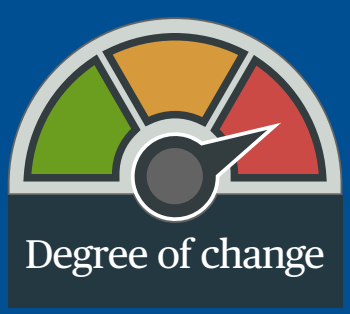
Where can I find this?

Article 4(4) & 20 *Recitals 71 & 72*

Data governance obligations

At a glance

- The GDPR requires all organisations to implement a wide range of measures to reduce the risk of their breaching the GDPR and to prove that they take data governance seriously.
- These include accountability measures such as: Privacy Impact Assessments, audits, policy reviews, activity records and (potentially) appointing a data protection officer a ("DPO").
- For those organisations which have not previously designated responsibility and budget for data protection compliance these requirements will impose a heavy burden.



To do list

☐	Assign responsibility and budget for data protection compliance within your organisation. Whether or not you decide to appoint a DPO (or have to) the GDPR's long list of data governance measures necessitates ownership for their adoption being allocated.
☐	Be clear as to whether those to whom you have designated responsibility are a DPO (for GDPR purposes) or not, given the special status afforded to DPOs by the GDPR.
☐	Consider reporting lines –supervisory authorities will expect a line direct to the board – and the job specification for those designated with data protection responsibilities.
☐	Ensure that a full compliance program is designed for your organisation incorporating features such as: PIAs, regular audits, HR policy reviews and updates and training and awareness raising programs.
☐	Audit existing supplier arrangements and update template RFP and procurement contracts to reflect the GDPR's data processor obligations.
☐	Monitor the publication of supervisory authorities / EU and industry published supplier terms and codes of practice to see if they are suitable for use by your organisation. If you are a supplier, consider the impact of the GDPR's provisions on your cost structure and responsibility for signing off the legality of your customer's activities.
☐	Implement measures to prepare records of your organisation's processing activities. If you are a supplier develop your strategy for dealing with customer requests for assisting with the development of such records.

The GDPR enshrines a number of "data governance" concepts the virtues of which law makers and supervisory authorities (DPOs) have extolled for some time. These concepts will create significant new operational obligations and costs for many public and private sector organisations.

A general obligation is imposed upon controllers to adopt technical and organisational measures to meet their GDPR obligations (and to be able to demonstrate that they have done so.) Operating a regular audit program, plus the other measures detailed below (PIAs in particular), seem likely to be regarded in a favourable light by supervisory authorities in their enforcement of the obligations of the GDPR.

Key obligations include the following:

Privacy by design

Organisations must implement technical and organisational measures to show that they have considered and integrated data compliance measures into their data processing activities.

Adopting appropriate staff policies is specifically mentioned, as is the use of pseudonymisation (to ensure compliance with data minimisation obligations).

Privacy Impact Assessments (PIAs)

A PIA is an assessment to identify and minimise non-compliance risks. The concept is not a new one – current regulator guidance recommends their use and Bird & Bird has run PIAs for a number of its clients – but the GDPR formalises a requirement for PIAs to be run.

Specifically, controllers must ensure that a PIA has been run on any *"high risk"* processing activity before it is commenced – measured by reference to the risk of infringing a natural person's rights and freedoms.

"Large scale" processing of sensitive data, or profiling activities are cited as (non-exhaustive) examples of high risk processing. Supervisory authorities are to publish details of further examples and guidance.

As a minimum, the GDPR requires that a PIA include:

- A description: of the processing activities and their purpose;
- An assessment: of the need for and proportionality of the processing, the risks arising and measures adopted to mitigate those risks, in particular safeguards and security measures to protect personal data and comply with the GDPR.

If a DPO has been appointed (see below), his/her advice on the carrying out of the PIA must be sought.

A supervisory authority must be consulted before any data processing commences if a PIA identifies a high level of unmitigated risk in certain circumstances. The GDPR contains specific procedural directions for this process.

Controllers are directed to seek the views of affected data subjects *"and their representatives"* in conducting a PIA, if appropriate. In the context of HR data processing this is likely to be interpreted as an obligation to consult with works councils or Trade Unions.

Data Protection Officer (DPO)

Controllers and processors are free to appoint a DPO but the following must do so:

- Public authorities (with some minor exceptions);
- Any organisation whose core activities require:
  - *"regular and systematic monitoring"* of data subjects *"on a large scale"*; or
  - *"large scale"* processing of Sensitive Data or criminal records; and
- Those obliged to do so by local law (countries such as Germany are likely to fall into this category).

Where appointed, DPOs must be selected by reference to their professional qualities and expert knowledge (which their employer is obliged to help them maintain).

Their tasks should as a minimum include: advising their colleagues and monitoring their organisation's GDPR/privacy law/policy compliance, including via training and awareness raising, running audits, advising regarding PIAs and co-operating with supervisory authorities.

Adequate resources must be provided to enable DPOs to meet their GDPR obligations, and they should report directly to the highest level of management.

Group companies can appoint a single DPO. A DPO can be a member of staff or a hired contractor.

Controllers and processors must ensure that the DPO can operate independently of instruction and is not dismissed or penalised for performing their task. It remains to be seen how the employment laws will interpret this provision.

The DPO's contact details must be published and also notified to an organisation's supervisory authority as the DPO is to be a point of contact for questions about data protection compliance matters.

Using service providers (data processors)

The GDPR imposes a high duty of care upon controllers in selecting their personal data processing service providers which will require procurement processes and request for tender documents to be regularly assessed.

Contracts must be implemented with service providers which include a range of information (e.g. the data processed and the duration for processing) and obligations (e.g. assistance where a security breach occurs, pseudonymisation and encryption measures taken and audit assistance obligations). Likewise where a service provider hires a sub-processor.

The Commission and supervisory authorities are likely to publish approved form service provider contract clauses. It seems likely that, from a service provider's point of view, these will be onerous. Providers' approach to pricing contracts will therefore need to be reviewed.

Record of processing activities

Organisations are obliged to keep a record of their processing activities (the type of data processed, the purposes for which it is used etc) similar to that which under current laws controllers are required to register with DPAs.

Data processors are also required to maintain such a record about personal data which controllers engage them to process, a requirement which will challenge many cloud and communications service providers.

Whilst an exemption from the above obligations applies to organisations employing fewer than 250 people this exemption will not apply where sensitive data are processed, which seems likely to nullify its usefulness.

Where can I find this?

Privacy by Design	*Article 25*	*Recitals 74-78*
PIAs	*Articles 35-36*	*Recitals 84 & 89-94*
DPOs	*Articles 37-39*	*Recital 97*
Using data processors	*Article 28*	*Recitals 80-81*
Record of processing activities	*Article 30*	*Recital 82*

Personal data breaches and notification

At a glance

- Data controllers and data processors are now subject to a general personal data breach notification regime.
- Data processors must report personal data breaches to data controllers.
- Data controllers must report personal data breaches to their supervisory authority and in some cases, affected data subjects, in each case following specific GDPR provisions.
- Data controllers must maintain an internal breach register.
- Non-compliance can lead to an administrative fine up to €10,000,000 or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- As things stand, the specific breach notification regime for communications service providers, set out in Commission Regulation 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC, still applies.

To do list

- ☐ In line with the accountability principle laid down by the GDPR, data controllers and data processors should develop or update their internal breach notification procedures, including incident identification systems and incident response plans.
- ☐ Such procedures should be regularly tested and re-reviewed.
- ☐ Work with your IT/IS teams to make sure they implement appropriate technical and organisational protections to render the data unintelligible in case of unauthorised access
- ☐ Insurance policies should be revisited to assess the extent of their coverage in case of breaches
- ☐ Template MSA/data protection clauses and tender documentation should be updated by customers, including: (i) to require suppliers to proactively notify breaches to them; and (ii) put a great emphasis on the duty to cooperate between the parties

Degree of change

Incidents which trigger notification

In case of an incident defined as, *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*, the new breach notification regime under the GDPR will apply as follows:

1. Obligation for data processors to notify data controllers

Timing:

Without undue delay after becoming aware of it

Exemption:

None in the GDPR (but EDPB tasked to issue guidelines on *"the particular circumstances in which a controller or a processor is required to notify the personal data breach"*)

Observations:

- All breaches will have to be reported.
- EDPB to issue guidelines to clarify the notion of "undue delay" and the particular circumstances in which a data processor is required to notify the personal data breach

2. Obligation for data controllers to notify the supervisory authority

Timing:

Without undue delay and, where feasible, not later than 72 hours after becoming aware of it

Exemption:

No reporting if the breach is unlikely to result in a risk for the rights and freedoms of natural persons

Observations:

- When the timing obligation is not met, reasons will have to be provided to the supervisory authority (e.g. request from a law enforcement authority)
- EDPB to issue guidelines to clarify the notion of "undue delay" and the particular circumstances in which a data controller is required to notify the personal data breach

3. Obligation for data controller to communicate a personal data breach to data subjects

If the data controller is yet to do so, the supervisory authority may compel the data controller to communicate a personal data breach with affected data subjects unless one of the three exemptions is satisfied

Timing:

Without undue delay: the need to mitigate an immediate risk of damage would call for a prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for communication.

Exemption:

No reporting if:

- The breach is unlikely to result in a high risk for the rights and freedoms of data subjects;
- Appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); or
- This would trigger disproportionate efforts (instead a public information campaign or "similar measures" should be relied on so that affected individuals can be effectively informed)

Documentation requirements

- Internal breach register: obligation for the data controller to document each incident *"comprising the facts relating to the personal data breach, its effects and the remedial action taken"*. The supervisory authority can be requested to assess how data controllers comply with their data breach notification obligations
- There are also prescribed requirements to satisfy in the communication to the supervisory authority (e.g. describing the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned, etc.) and the communication to affected individuals (e.g. describe in clear and plain language the nature of the personal data breach and provide at least the following information: (i) the name and contact details of the data protection officer or other contact point where more information can be obtained; (ii) the likely consequences of the personal data breach; and (iii) the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects).

Sanctions in case of non-compliance

Failure to meet the above requirements exposes the organisation to an administrative fine of up to €10,000,000 or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

What about the other EU breach notification regime for communications service providers?

As things stand, Regulation 611/2013 – which details a specific procedure for breach notification (laid out in Directive 2002/58/EC (the "e-Privacy Directive") as amended) - still applies to providers of publicly available telecommunications services (e.g. telecommunication companies, ISPs and email providers). It remains to be seen whether the revision of the e-Privacy Directive announced by the Commission in the course of 2016 will trigger an alignment, or the persistence of, the two breach notification regimes.

Where can I find this?

Recitals 85-88 *Articles 33, 34, 70, 83 & 84*

Codes of conduct and certifications

At a glance

The GDPR makes provision for the approval of codes of conduct ("Codes") and the accreditation of certifications, seals and marks to help controllers and processors demonstrate compliance and best practice.

Codes of conduct:

- Associations and representative bodies may prepare Codes for approval, registration and publication by a supervisory authority, or, where processing activities take place across member states, by the European Data Protection Board ("EDPB"). The EU Commission may declare Codes recommended by EDPB to have general validity within the EU.
- Codes may be approved in relation to a wide range of topics and adherence to Codes will help controllers and processors demonstrate compliance with GDPR obligations.
- Compliance with Codes will be subject to monitoring, which may be carried out by suitably qualified, accredited bodies. Controllers and processors who are found to have infringed a relevant code may be suspended from participation in the Code and reported to the supervisory authority.

Certifications, seals and marks:

- The establishment of data protection certification mechanisms and of seals and marks is to be encouraged
- Certificates will be issued by accredited certifying bodies (yet to be established).
- Certification is voluntary but certification will enable controllers and processors to demonstrate compliance with the GDPR.
- Certificates will be valid for three years and subject to renewal.
- EDPB will maintain a publicly available register of all certification mechanisms, seals and marks.

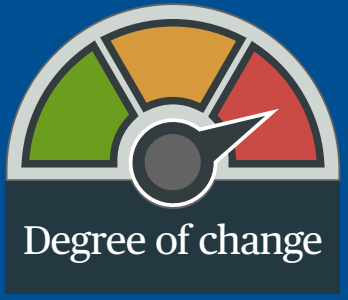
To do list

Codes of Conduct

- In order to get a head-start before the accreditation procedures are laid out by the supervisory authorities, processors (such as cloud providers) and controllers within specific sectors should consider identifying, or establishing, associations or representative bodies that could develop Codes for approval by supervisory authorities.

Certification, seals and marks

- Processors and controllers should follow developments in relation to the accreditation of certification bodies, and consider whether they will wish to apply for certification in due course.
- Once certification schemes are established, controllers should familiarise themselves with relevant schemes and take account of certifications, seals and marks when selecting their processors/ service providers



Codes of conduct

Codes are an important component in broadening and adapting the tools for data protection compliance that controllers and processors can draw on, by way of a *"semi-self-regulating"* mechanism.

It is expected that Codes will provide authoritative guidance on certain key areas including:

- legitimate interest in specific contexts;
- pseudonymisation;
- exercise of data subjects' rights;
- protection of minors and modes of parental consent;
- proper implementation of privacy by design and by default, and security measures;
- security breach notification; and
- dispute resolution between controllers and data subjects.

The development and the approval of Codes are likely to deliver a number of benefits including:

- establishing and updating best practice for compliance in specific processing contexts;
- enabling data controllers and processors to commit to compliance with recognised standards and practices and be recognised for doing so;
- adherence to Codes can demonstrate that data importers (controllers as well as processors) located outside the EU / EEA have implemented adequate safeguards in order to permit transfers under Article 46; transfers made on the basis of an approved code of conduct together with binding and enforceable commitments of the importer to apply appropriate safeguards may take place without any specific authorisation from a supervisory authority and Codes may therefore offer an alternative mechanism for managing international transfers, standing on the same level as standard contractual clauses and BCR.

Approval of Codes

Codes proposed by associations or representative bodies in relation to data processing activities that affect only one member state are to be submitted to the competent supervisory authority, for comment and – subject to possible modifications or extensions – approval. If a Code covers processing operations in several Member States, it should be submitted to the EDPB for an opinion. Subject to possible modifications or extensions, the Code and the EDPB opinion may then be submitted to the European Commission which, upon due examination, may declare its general validity.

Codes are to be kept and made available in publicly accessible registers.

Monitoring of compliance

Monitoring of compliance with Codes will be carried out only by bodies accredited by the competent supervisory authority.

In order to become accredited such bodies will have to demonstrate:

- their independence and expertise;
- that they have established procedures to assess the ability of controllers and processors to apply the Code, and to monitor compliance, as well as periodically review the Code;
- the ability to deal with complaints about infringements; and
- that they have processes in place to avoid conflicts of interest.

Accreditations are revocable if the conditions for the accreditation are no longer met.

Certifications, seals and marks

The concept of certifying data processing operations is a significant development in creating a reliable and auditable framework for data processing operations. It is likely to be particularly relevant in the context of cloud computing and other forms of multi-tenancy services, where individual audits are often not feasible in practice.

Member States, supervisory authorities, the EDPB and the Commission are all encouraged to establish data protection certification mechanisms, seals and marks, with regard to specified processing operations.

Certifications are voluntary. The competent supervisory authority or the EDPB will approve criteria for the certifications. The EDPB may develop criteria for a common certification, the European Data Protection Seal.

There are two key advantages of certificates:

1. controllers and processors will be able to demonstrate compliance, in particular with regard to implementing technical and organisational measures.

2. certificates can demonstrate that data importers (controllers as well as processors) located outside the EU / EEA have implemented adequate safeguards for the purpose of Article 46; transfers made on the basis of an approved certification mechanism together with binding and enforceable commitments of the importer to apply appropriate safeguards may take place without any specific authorisation from a supervisory authority and certificates therefore offer an alternative mechanism for managing international transfers, standing on the same level as standard contractual clauses and BCR.

Certificates on processing operations will be issued for a period of three years, and are subject to renewal or withdrawal where the conditions for issuing the certificate are no longer met.

The EDPB is to maintain a publicly available register with all certification mechanisms, data protections seals and marks.

Certificates can be issued by – private or public - accredited certification bodies. National Accreditation Bodies and/or supervisory authorities may accredit certification bodies (so that they can issue certificates, marks and seals), that (*inter alia*):

- have the required expertise and is independent in regard to the subject matter of certification;
- have procedures to review and withdraw certifications, seals and marks;
- are able to deal with complaints about infringements of the certifications; and
- have rules to deal with conflicts of interest.

Criteria for accreditation will be developed by the supervisory authorities or the EDPB and will be publicly available.

Accreditations for certification bodies will be issued for a maximum of five years and are subject to renewals, as well as withdrawals in cases where conditions for the accreditation are no longer met.

Where can I find this?

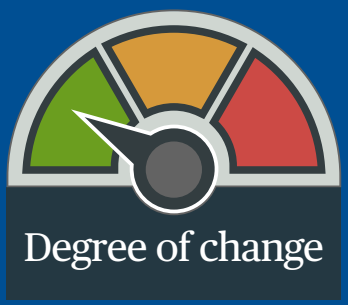
Codes of conduct
Articles 24, 32, 40, 41, 57, 58, 64, 70, 83
Recitals 77, 81, 98, 99, 148, 168

Certifications, seals and marks
Articles 24, 25, 28, 32, 40, 42, 43
Recitals 46, 57, 58, 64, 70, 83

Transfers of personal data

At a glance

- Transfers of personal data to recipients in "third countries" (i.e. outside of the European Economic Area ("EEA")) continue to be regulated and restricted in certain circumstances.
- The GDPR's obligations are broadly similar to those imposed by the Data Protection Directive, with some compliance mechanism improvements available, notably the removal of the need to notify standard contract clauses to supervisory authorities, and encouragement for the development of transfer adequacy codes of practice and certification schemes.
- Data transfer compliance will remain a significant issue for multinational organisations and also for anyone using supply chains which process personal data outside the EEA.
- Breach of the GDPR's data transfer provisions is identified in the band of non-compliance issues for which the maximum level of fines can be imposed (up to 4% of worldwide annual turnover).
- Non-compliance proceedings can be brought against controllers and/or processors.



To do list

☐	Review and map key international data flows.
☐	Consider what data transfer mechanisms you have in place and whether these will continue to be appropriate.
☐	Review questions included in standard procurement templates and contract clauses to ensure that information about your supplier's proposed transfer of personal data for which you are responsible is understood and conducted in a compliant way.
☐	If you or your suppliers previously relied upon a Safe Harbor certification to ensure adequacy, this is no longer valid. You will need to re-evaluate your relationships with service providers and/or customers to establish the new legal basis that will justify on-going transatlantic data transfers.
☐	For intra group data transfers, consider whether BCRs would be a viable option.
☐	If you transfer personal data outside the EEA whilst supplying goods or services, expect to be questioned by customers about your (and your supplier's) approach to transfer compliance.
☐	Keep an eye on developments regarding approved codes of conduct and certification schemes carried out in the context of an organisation's activities.

Commentary

Transfers of personal data to "third countries" (i.e. outside of the EEA) continue to be restricted under the GDPR. This will remain a significant issue for any multinational organisation. However, the current requirements will broadly remain in place, with some improvements.

The main improvement is that the current process, whereby transfers based on standard contractual clauses have to be notified to or approved by data protection authorities, is abolished.

The Commission will have the power to determine that certain countries, territories, specified sectors or international organisations offer an adequate level of protection for data transfers. The existing list of countries which have previously been approved by the Commission will remain in force, namely: Andorra, Argentina, Canada (where PIPEDA applies), Switzerland, Faero Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand. Countries to be added to or taken off this list shall be published in the Official Journal.

The US safe harbor scheme which was previously approved by the Commission is no longer valid. Discussions to replace Safe Harbor with the EU-US Privacy Shield are, at the date of publication, ongoing. These discussions are not referenced in the GDPR, although the GDPR does incorporate the key requirements assessing adequacy, as set out in the Schrems decision.

The GDPR provides more detail on the particular procedures and criteria that the Commission should consider when determining adequacy, stressing the need to ensure that the third country offers levels of protection that are *"essentially equivalent to that ensured within the Union"*, and providing data subjects with effective and enforceable rights and means of redress. The Commission shall consult with the EDPB when assessing levels of protection and ensure that there is on-going monitoring and review of any adequacy decisions made (at least every four years). The Commission also has the power to repeal, amend or suspend any adequacy decisions.

Other existing methods of transferring personal data continue to be recognised: Standard contractual clauses (either adopted by the Commission or adopted by a supervisory authority and approved by the Commission) will remain an option and the existing sets of approved clauses will remain in force.

The use of other appropriate safeguards, such as binding corporate rules (BCRs) and legally binding and enforceable instruments between public authorities, will also be accepted.

Significantly, transfers will be permitted where an approved code of conduct (based on the new scheme in Article 40) or an approved certification mechanism (based on the new scheme in Article 42) is used, provided that binding and enforceable commitments are made by the controller or processor in the third country to apply the appropriate safeguards, including as regards the data subjects' rights. There are also provisions for ad hoc safeguards to be agreed, subject to authorisation from the competent supervisory authority.

With respect to BCRs, the GDPR writes into law the current requirements for BCRs for controllers and processors. These will still require approval from the competent supervisory authority but this has to be determined in accordance with a consistency mechanism. This will be helpful in those few Member States which are still not able to accept BCRs.

There continue to be a number of derogations permitting transfers of personal data in limited circumstances, which are similar to existing derogations, and include: explicit consent, contractual necessity, important reasons of public interest, legal claims, vital interests, and public register data. There is also a new (limited) derogation for non-repetitive transfers involving a limited number of data subjects where the transfer is necessary for compelling legitimate interests of the controllers (which are not overridden by the interests or rights of the data subject) and where the controller has assessed (and documented) all the circumstances surrounding the data transfer and concluded there is adequacy. The controller must inform the supervisory authority and the data subjects when relying on this derogation.

Finally, as widely expected, the GDPR makes it clear that it is not lawful to transfer personal data outside the EEA in response to a legal requirement from a third country, unless the requirement is based on an international agreement or one of the other grounds for transfer applies. The UK has opted out of this provision.

Where can I find this?

Articles 40-45, Recitals 78-91

Appointment of supervisory authorities

At a glance

- National data protection authorities will continue to exist.
- They must co-operate together and with the European Commission and monitor the application of the GDPR.
- They must act independently.
- Members of supervisory authorities must be appointed in a publicly transparent way and be skilled in data protection.

To do list

No action is required (unless perhaps you are a member of an existing data protection authority or its staff!)

Commentary

National data protection authorities, (supervisory authorities) will continue to exist. They are to monitor the application of the GDPR to protect fundamental rights in relation to processing and to facilitate the free flow of personal data within the EU.

They have to co-operate with each other and the European Commission in order to contribute to the consistent application of the GDPR.

States such as Germany can keep more than one supervisory authority, but one of them has to be nominated as the representative on the new European Data Protection Board ("EDPB").

The Commission must be notified of national laws on the setting up and appointment of supervisory authorities.

Supervisory authorities are to act with complete independence (but subject to financial auditing and judicial supervision). Members of supervisory authorities are to stay free from external influence and neither seek nor take instructions from anyone. They must not act incompatibly with their duties nor, whilst in office, engage in an incompatible occupation, whether or not gainful.

Member States must provide their supervisory authorities with the human, technical, financial and other resources necessary to carry out all their tasks and exercise their powers effectively.

Each supervisory authority is to choose its own staff and have sole direction of them. A supervisory authority's budget is to be public and separately identified, even if part of the national budget.

Member State law is to establish the supervisory authorities, prescribe the rules for their members, their qualifications and eligibility. Their term of office is to be not less than four years and member States can make that renewable. Members' duties of independence outlined above must be embodied in national law. Members of supervisory authorities and their staff are bound by a duty of *"professional secrecy"* both when in office and subsequently.

These provisions on setting up supervisory authorities are a more detailed elaboration of the provisions found in Article 28 of the old framework Data Protection Directive 95/46/EC. There is nothing strikingly unusual in the new rules. Some points, however, are worth remarking on: the specificity of the term of appointment, the emphasis on independence, the insistence on the provision of adequate resources for each supervisory authority, and the requirement that *"each member [of supervisory authorities] shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers."*

There are likely to be disputes about whether supervisory authorities are adequately funded, particularly in cases such as the UK where the traditional source of funding from registration/ notification fees will cease.

Where can I find this?

Recitals 117-123, Chapter VI Section 1, Articles 51-54

Competence, tasks and powers

At a glance

- Supervisory authorities are given specific competence to act on their own territory.
- A lead-authority has competence in cross-border cases (see section on co-operation and consistency between supervisory authorities for further details).
- Supervisory authorities are given an extensive list of specific powers and tasks.

To do list

- ☐ Familiarise yourself with the comprehensive powers and tasks of the supervisory authorities.
- ☐ If you carry out cross-border processing, get to understand the lead-authority system, (for which see section on cooperation and consistency between supervisory authorities).
- ☐ You might wish to consider working towards compliance with a recognised Code of Conduct or Certification which will require supervisory authority approval.

Competence

Supervisory authorities (also colloquially known as "Data Protection Authorities" or "DPAs") are given competence *"for the performance of the tasks assigned to and the exercise of the powers conferred on it"* described in the GDPR on their natural territory. Recital 122 tells us that this competence includes *"processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing in its territory"*.

In cases where the legal basis for processing, whether by a private body or a public authority, is a legal obligation, acting in the public interest or in the exercise of official authority, the 'concerned' authority has competence and the cross-border lead authority system is disapplied. The language is rather obscure, but Recital 128 says that a supervisory authority has exclusive jurisdiction over both public authorities and private bodies acting in the public interest which in either case are established on the supervisory authority's territory. It is not clear whether this contemplates multiple establishments and is a means of excluding the one-stop shop or whether it gives exclusive jurisdiction to the home supervisory authority even if the processing is elsewhere in the EU. This might have wide application to private sector bodies – e.g. financial institutions carrying out anti-money-laundering activities in relation to customers elsewhere in the EU than the home country.

Supervisory authorities cannot exercise jurisdiction over courts acting in a judicial capacity. 'Court' is not defined and it is not entirely clear how far down the judicial hierarchy this rule will extend.

A lead-authority system is set up to deal with cross-border processing (see section on co-operation and consistency between supervisory authorities for further information about this complex arrangement).

Tasks

There is a very comprehensive list of tasks given to the supervisory authorities by Article 57 of the GDPR. There is no need to list them all, because the last on the list is *"fulfil any other tasks related to the protection of personal data"*. Supervisory authorities must therefore do anything that might reasonably be said to be about the *"protection of personal data"*.

Where can I find this?

Recitals 117-123, Chapter VI Section 2 Articles 55-59

Some tasks are worth emphasising. Supervisory authorities are to monitor and enforce the *"application"* of the GDPR and to promote awareness amongst the public, controllers and processors.

They are to advise their governments and parliaments on proposed new laws.

Helping data subjects, dealing with and investigating complaints lodged by individuals or representative bodies, conducting investigations and especially co-operating with other supervisory authorities are all specifically mentioned, as is monitoring the development of technical and commercial practices in information technology.

Supervisory authorities are to encourage the development of Codes of Conduct and Certification systems and they are to *"draft and publish the criteria for accreditation"* of certification bodies and those which monitor codes of conduct.

Supervisory authorities cannot charge data subjects or Data Protection Officers for their services; the GDPR is however silent on whether controllers and processors could be charged fees in respect of services they receive from supervisory authorities.

Powers

Article 58 of the GDPR lists the powers of the supervisory authorities to which Member States can add if they wish. Many of the powers correspond to the specific tasks listed in Article 57 and do not need repeating.

Worthy of mention are: ordering a controller or processor to provide information; conducting investigatory audits; obtaining access to premises and data; issuing warnings and reprimands and imposing fines; ordering controllers and processors to comply with the GDPR and data subjects' rights; banning processing and trans-border data flows outside the EU; approving standard contractual clauses and binding corporate rules. The exercise of powers by a supervisory authority must be subject to safeguards and open to judicial challenge.

Member States must give supervisory authorities the right to bring matters to judicial notice and *"where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation"*. Presumably the existing variation in powers will continue in accordance with national law and procedure.

Finally, supervisory authorities must produce annual reports. In summary, the competence, powers and tasks of supervisory authorities are a comprehensive listing of everything a supervisory authority must or might do. This is largely a predictable consolidation of existing practices with some innovations in individual Member States.

Co-operation and consistency between supervisory authorities

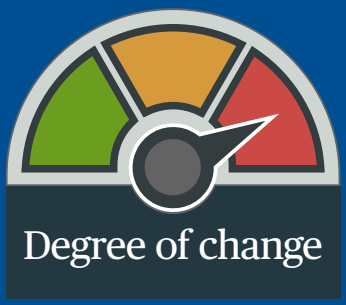
At a glance

In cases of cross-border processing in the EU, the European Commission proposed a one-stop shop whereby the supervisory authority for the main establishment of the controller, would be the sole authority for monitoring and ensuring compliance by that controller throughout the EU. In the face of strong opposition, that has been watered down.

There will now be a lead authority in cases of multiple establishments or cross-border processing in the EU, which will be the supervisory authority for the main establishment, butsupervisory authorities in other countries where that controller is established, or where data subjects are significantly affected, or authorities to whom a complaint has been made, can be involved in cases, and the lead authority must co-operate with them. Non-leading authorities can also handle purely local cases involving a cross-border controller.

To do list

- ☐ If you carry out activities within just a single Member State – (as is still true for the majority of businesses), the lead authority system is irrelevant and the dispute mechanism is only likely to affect you if a relevant proposed Code of Conduct or Certification System is delayed or opposed by the EDPB.
- ☐ If you carry out activities in two or more member states, find out who your lead authority might be and engage with that authority in the run up to implementation by for example accessing training and guidance it makes available.



Commentary

Lead Authority Competence

If a controller or processor carries out cross-border processing either through multiple establishments in the EU or even with only a single establishment, the supervisory authority for the main or single establishment acts as lead authority in respect of that cross-border processing.

A national supervisory authority remains competent to exercise powers if a complaint is made to it or an infringement occurs on its territory and if the subject matter of the complaint or infringement relates only to an establishment on that territory or substantially affects data subjects only in that State. The European Data Protection Board ("EDPB") can give guidance on what is meant by *"substantially"* affecting data subjects in more than one Member State.

Such local cases have to be notified to the lead authority which has three weeks to decide whether to intervene (taking into account whether there is an establishment in the other state) and then apply the co-operation procedure. Non-lead authorities can propose decisions to the lead authority.

If the lead authority does not intervene, the local authority handles the case using, where necessary, the mutual assistance and joint investigation powers.

Co-operation Procedure

The lead authority has to co-operate with other "concerned" supervisory authorities. They have to exchange information and try to reach consensus.

The lead authority has to provide information to the other supervisory authorities and it can seek mutual assistance from them and conduct joint investigations with them on their territories. The lead authority must submit a draft decision to concerned authorities without delay and they have four weeks in which to object. There can be another round of submitting draft decisions with a two week objection period. If the lead authority does not wish to follow the views of concerned authorities it must submit to the consistency procedure supervised by the EDPB.

There are detailed rules about which supervisory authority should take the formal decision and notify the controller, but the lead authority has the duty to ensure that, pursuant to a formal decision, compliance action is taken by a controller in all its establishments.

A lead authority can exceptionally, however, take urgent temporary action without waiting to complete the consistency process.

The lead authority system has a number of apparent weaknesses and could be undermined where non-lead authorities are able to assert themselves on the grounds that data subjects in their jurisdictions are substantially affected by processing conducted by a controller whose main establishment is elsewhere; its success will rely to a large extent on consensus and good will between supervisory authorities.

Mutual Assistance, Joint Operations & Consistency

Supervisory authorities are required to provide assistance to each other in the form of information or carrying out *"prior authorisations and consultations, inspections and investigations"*. The European Commission can specify forms and procedures for mutual assistance.

Supervisory authorities can conduct joint investigation and enforcement operations. A supervisory authority has a right to be included in such operations if a controller has an establishment on its territory or a significant number of its data subjects are likely to be substantially affected. If local law permits, a host supervisory authority can give formal investigatory powers to seconded staff. Supervisory authorities have conducted joint investigations under the existing law, so the GDPR in practice will probably just develop and strengthen these arrangements.

Where supervisory authorities take certain formal steps or disagree or wish for action to be taken by another supervisory authority, the GDPR provides for a consistency and dispute resolution mechanism.

The EDPB has to give opinions on various supervisory authority proposals, including the approval of binding corporate rules, certification criteria and codes of conduct. If the supervisory authority disagrees with an EDPB opinion, the matter goes to the dispute resolution procedure.

That procedure also applies to lead authority/concerned authority disputes. In all these cases, the EDPB takes a binding decision on the basis of a two-thirds majority vote. If there is no such majority, then after a delay, a simple majority will suffice. The supervisory authorities involved are bound to comply and formal decisions have to be issued in compliance with the EDPB decision.

Where can I find this?

Recitals 124-138 and Chapter VII, Sections 1 & 2

European Data Protection Board

At a glance

- The old Article 29 Working Party, whose members were the EU's national supervisory authorities, the European Data Protection Supervisor ("EDPS") and the European Commission, has been transformed into the "European Data Protection Board" ("EDPB"), with similar membership but an independent Secretariat.
- The EDPB has the status of an EU body with legal personality and extensive powers to determine disputes between national supervisory authorities, to give advice and guidance and to approve EU-wide codes and certification.

To do list

- ☒ No immediate action is essential – unless perhaps you are a member of a national supervisory authority.
- ☐ Nevertheless, the EDPB will be a major influence on EU Data Protection law and practice and you may wish to learn how to influence or challenge its decisions.

Degree of change

Commentary

The Article 29 Working Party, which was established by Directive 95/46/EC (the "Data Protection Directive") and consists of representatives from EU Member State supervisory authorities together with the Commission and the EDPS, will be abolished by the GDPR. It is to be replaced by the EDPB, which will similarly be made up of the heads of national supervisory authorities (or their representatives) and the EDPS.

The Commission representative on the EDPB is a non-voting member and in states (such as Germany) with multiple supervisory authorities, the national law must arrange for a joint representative to be appointed. In dispute resolution cases, where a binding decision is to be given, the EDPS's voting powers are restricted to circumstances in which the principles of the case would be applicable to the EU institutions.

The EDPB has a much enhanced status. It is not merely an advisory committee, but an independent body of the European Union with its own legal personality.

It is formally represented by its Chair, who has the chief role in organising the work of the EDPB and particularly in administering the conciliation procedure for disputes between national supervisory authorities. The Chair and two Deputies are elected from the membership of the EDPB and serve for five years, renewable once.

The EDPB normally decides matters by a simple majority, but rules of procedure and binding decisions (in the first instance) are to be determined by a two-thirds majority.

The EDPB is to adopt its own rules of procedure and organise its own affairs. The independence of the EDPB is emphasised. There seems to be an implicit suggestion that the Commission has exercised too great an influence over the Article 29 Working Party in the past and was seeking to consolidate this power.

The Secretary to the old Article 29 Working Party was a Commission official. The new EDPB will have its own Secretariat provided by the EDPS, but which acts solely under the direction of the chair of the EDPB.

The EDPB is given a long and detailed list of tasks, but its primary role is to contribute to the consistent application of the GDPR throughout the Union. It advises the Commission, in particular on the level of protection offered by third countries or international organisations, and promotes cooperation between national supervisory authorities. It issues guidelines, recommendations and statements of best practice: for example, on matters such as when a data breach is *"likely to result in a high risk to the rights and freedoms"* of individuals or on the requirements for Binding Corporate Rules. It is to encourage Codes of Practice and Certification, both of which will assist controllers and processors in demonstrating compliance with the GDPR.

Much of this list of tasks is an elaboration or formalisation of the activity of the current Article 29 Working Party, but the views and activities of the EDPB will have greater force and effect.

The EDPB's most distinctive new role is to conciliate and determine disputes between national supervisory authorities. For more about that activity, see the section on competence, tasks and powers. The old Article 29 Working Party was often criticised for not consulting adequately before taking decisions. The new EDPB is required to consult interested parties *"where appropriate"*. Notwithstanding the "get-out" qualification, this is a major benefit to those who may be affected by opinions, guidelines, advice and proposed best practice.

EDPB discussions are to be *"confidential where the Board deems it necessary, as provided for in its rules of procedure"*. This suggests that meetings and discussions will, in principle, be public unless otherwise determined.

Finally, the EDPB has to prepare an Annual Report.

Where can I find this?

Recitals 139 & 140, and Chapter VII Section 3

Remedies and liabilities

At a glance

- Individuals have the following rights (against controllers and processors):
  - the right to lodge a complaint with supervisory authorities where their data have been processed in a way that does not comply with the GDPR;
  - the right to an effective judicial remedy where a competent supervisory authority fails to deal properly with a complaint;
  - the right to an effective judicial remedy against a relevant controller or processor; and
  - the right to compensation from a relevant controller or processor for material or immaterial damage resulting from infringement of the GDPR.
- Both natural and legal persons have the right of appeal to national courts against a legally binding decision concerning them made by a supervisory authority.
- Individuals can bring claims for non-pecuniary loss, not just for compensation. The potential for group actions to be brought is facilitated.

To do list

- Controllers and their processors should ensure that data processing agreements and contract management arrangements clearly specify the scope of the processor's responsibilities and should agree mechanisms for resolving disputes regarding respective liabilities to settle compensation claims.
- Controllers and processors should agree to report to other controllers or processors that are involved in the same processing, any relevant compliance breaches and any complaints or claims received from relevant data subjects.
- Joint data controllers should agree their respective obligations for data protection compliance, their respective liabilities for data protection breaches and mechanisms for resolving disputes regarding respective liabilities to settle compensation claims.

Degree of change

Complaints to supervisory authorities

Data subject rights to complain to supervisory authorities are slightly strengthened as compared to the Data Protection Directive. The Directive obliges supervisory authorities to hear claims lodged by data subjects for checks on the lawfulness of data processing and to inform data subjects that a check has taken place.

Under the GDPR, data subjects whose personal data are processed in a way that does not comply with the GDPR have a specific right to lodge a complaint with supervisory authorities and supervisory authorities must inform data subjects of the progress and outcome of complaints lodged.

Judicial remedies against decisions of supervisory authorities

Both data subjects and other affected parties have rights to an effective judicial remedy in relation to certain acts and decisions of supervisory authorities.

- Any person has the right to an effective judicial remedy against legally binding decisions concerning him/her, taken by a supervisory authority.
- Data subjects have the right to an effective judicial remedy where a supervisory authority fails to deal with a complaint or fails to inform the data subject within 3 months on progress or outcome of his or her complaint.

Recital 143 explains that decisions and actions that may be challenged in the courts include the exercise of investigative, corrective, and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. The right does not encompass other measures by supervisory authorities which are not legally binding, such as opinions issued or advice provided by supervisory authorities.

Judicial remedies against data controllers & data processors

Data subjects whose rights have been infringed have the right to an effective judicial remedy against the data controller or processor responsible for the alleged breach. The Data Protection Directive makes equivalent provision for a judicial remedy against data controllers but not against data processors.

Liability for compensation

Any person who has suffered damage as a result of infringement of the GDPR has the right to receive compensation from the controller or the processor. Under the Data Protection Directive, liability for compensation is limited to controllers only.

The following provision is made for the allocation of liability for compensation between controllers and processors:

- controllers are liable for damage caused by processing which is not in compliance with the GDPR;
- processors are liable only for damage caused by processing in breach of obligations specifically imposed on processors by the GDPR, or caused by processing that is outside, or contrary to lawful instructions of the controller; and
- in order to ensure effective compensation for data subjects, controllers and processors that are involved in the same processing and are responsible for any damage caused, each shall be held liable for the entire damage. However, a processor or controller that is held liable to pay compensation on this basis is entitled to recover from other relevant parties, that part of the compensation corresponding to their part of the responsibility for the damage.

Whilst the Data Protection Directive refers only to the right to compensation for *"damage"*, the GDPR makes clear that compensation may be recovered for both pecuniary and non-pecuniary losses. This clarification is, however, consistent with current English law interpretation of the meaning of damage for the purpose of compensation claims under the Data Protection Act (see Google Inc. v Vidal-Hall & Others [2015] EWCA Civ 311) although the case is subject to appeal.

The GDPR provides that controllers and processors are exempt from liability if they are *"not in any way responsible for the event giving rise to the damage"*. This exemption appears to be slightly narrower than the exemption that can be claimed under the Data Protection Directive by a controller who can prove *"that he is not responsible for the event giving rise to the damage"*.

« Back to Table of Contents

Representative bodies

The GDPR entitles data subjects to mandate properly constituted representative bodies to lodge complaints with supervisory authorities on their behalf and to seek judicial remedies on their behalf against decisions of supervisory authorities or against data controllers or processors. The provision applies to representative bodies that are:

- properly constituted according to Member State law;
- a not-for-profit body, organisation or association;
- with statutory objectives that are in the public interest; and
- active in the field of data protection.

Data subjects may also mandate such bodies to exercise on their behalf rights to recover compensation from controllers or processors provided this is permitted by Member State law.

Where empowered to do so by Member State law, such representative bodies may, independently of the data subject's mandate, lodge complaints with supervisory authorities and seek judicial remedies against decisions of the supervisory authority or against data controllers or processors

There is no equivalent provision in the Data Protection Directive.

Where can I find this?

Articles 77-82 *Recitals 141-148*

Administrative fines

At a glance

- Supervisory authorities are empowered to impose significant administrative fines on both data controllers and data processors.
- Fines may be imposed instead of, or in addition to, measures that may be ordered by supervisory authorities. They may be imposed for a wide range of contraventions, including purely procedural infringements.
- Administrative fines are discretionary rather than mandatory; they must be imposed on a case by case basis and must be *"effective, proportionate and dissuasive"*.
- There are two tiers of administrative fines:
  - Some contraventions will be subject to administrative fines of up to €10,000,000 or, in the case of undertakings, 2% of global turnover, whichever is the higher.
  - Others will be subject to administrative fines of up to €20,000,000 or, in the case of undertakings, 4% of global turnover, whichever is the higher.
- Member States may determine whether, and to what extent public authorities should be subject to administrative fines.

To do list

- ☐ Run a GDPR compliance gap analysis to identify areas of most material non-compliance and to prioritise mitigating steps, especially in relation to high risk processing activities.
- ☐ Update risk registers.
- ☐ Assess liability exposure under existing customer, supplier and/or partner arrangements, including by assessing contract liability limitation and exclusion clauses.
- ☐ Review insurance arrangements.

Degree of change

General considerations

Administrative fines are not applicable automatically and are to be imposed on a case by case basis. Recital 148 clarifies that in the case of a minor infringement, or where a fine would impose a disproportionate burden on a natural person, a reprimand may be issued instead of a fine.

There is currently a high degree of variation across Member States in relation to the imposition of financial penalties by supervisory authorities. Although arrangements under the GDPR make provision for maximum penalties and allow supervisory authorities a degree of discretion in relation to their imposition, Recital 150 indicates that the consistency mechanism may be used to promote a consistent application of administrative fines.

Each Member States may however lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

Maximum administrative fines

The GDPR sets out two sets of maximum thresholds for administrative fines that may be imposed for relevant infringements.

In each case, the maximum fine is expressed in € or, in the case of undertakings, as a percentage of total worldwide annual turnover of the preceding year, whichever is higher. Recital 150 confirms that in this context *"an undertaking"* should be understood as defined in Articles 101 and 102 of the Treaty on the Functioning of the European Union ("TFEU") (i.e. broadly speaking, as entities engaged in economic activity).

Infringement of the following GDPR provisions are subject to administrative fines up to €20,000,000 or in the case of undertakings, up to 4% of global turnover, whichever is higher:

- the basic principles for processing, including conditions for consent (Articles 5, 6, 7 and 9);
- data subjects' rights (Articles 20-22);
- international transfers (Articles 44-49);
- obligations under Member State laws adopted under Chapter IX; and
- non-compliance with an order imposed by supervisory authorities (as referred to in Article 58(2)).

Other infringements are subject to administrative fines up to €10,000,000 or, in the case of undertakings, up to 2% of global turnover, whichever is higher. Contraventions subject to these maximum fines include infringement of the following obligations:

- to obtain consent to the processing of data relating to children (Article 8);
- to implement technical and organisational measures to ensure data protection by design and default (Article 25);
- on joint controllers to agree their respective compliance obligations (Article 26);
- on controllers and processors not established in the EU to designate representatives (Article 27);
- on controllers in relation to the engagement of processors (Article 28);
- on processors to subcontract only with the prior consent of the controller and to process data only on the controller's instruction (Articles 28-29);
- to maintain written records (Article 30);
- on controllers and processors to co-operate with supervisory authorities (Article 31);
- to implement technical and organisational measures (Article 32);
- to report breaches when required by the GDPR to do so (Articles 33-34);
- in relation to the conduct of privacy impact assessment (Articles 35-36);
- in relation to the appointment of Data Protection Officers (Articles 37-39);
- imposed on certification bodies (Article 42); and
- imposed on monitoring bodies to take action for infringement of codes of conduct (Article 41).

In cases where the same or linked processing involves violation of several provisions of the GDPR, fines may not exceed the amount specified for the most serious infringement.

« Back to Table of Contents

Factors to be taken into account

GDPR Article 83(2) lists factors to be taken into account when determining whether to impose an administrative fine and deciding on the amount of any fine to be imposed. These include:

- the nature, gravity and duration of the infringement having regard to the nature, scope or purpose of the processing concerned as well as the number of data subjects and level of damage suffered by them;
- whether the infringement is intentional or negligent;
- actions taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor;
- any relevant previous infringements;
- the degree of co-operation with the supervisory authority;
- categories of personal data affected;
- whether the infringement was notified by the controller or processor to the supervisory authority;
- any previous history of enforcement action;
- adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39; and
- any other aggravating or mitigating factors applicable in the circumstances e.g. financial benefits gained, losses avoided, directly or indirectly, from the infringement.

Where fines are imposed on persons that are not an undertaking, the supervisory authority should also take account of general income levels in the Member State as well as the economic situation of the person, in considering the appropriate amount of fine.

Where can I find this?

Article 83 *Recitals 148-151*

Derogations and special conditions

At a glance

Member States retain the ability to introduce derogations where these are required for the purposes of national security, prevention and detection of crime and in certain other situations. In line with case law of the Court of Justice of the European Union, any such derogation must respect *"the essence"* of the right to data protection and be a necessary and proportionate measure.

For these special purposes, the Regulation either requires or permits Member States to introduce supplemental laws. In the case of historical and scientific research, statistical processing and archiving, this can even provide a lawful basis for processing sensitive data.

Other special topics where Member State law is foreseen include processing of employee data, processing in connection with freedom of expression and professional secrecy (where restrictions of supervisory authority audit rights are foreseen).

Controllers (and, in some cases, processors) will need to check for and adjust to different Member State approaches in these areas.

To do list

- ☐ Assess whether any processing you carry out may be subject to derogations or special conditions under the GDPR.
- ☐ Where a derogation or special condition may apply to your processing, establish the jurisdictions in which this processing takes place.
- ☐ Consider further lobbying work in countries where you may be affected by the introduction of local restrictions.
- ☐ Where professional secrecy rules apply to any personal data received or obtained by a controller or processor, ensure these are appropriately marked so they can be protected from disclosure to supervisory authorities

Degree of change

Unknown – Many of the same categories of derogations and special conditions apply as provided for in Directive 95/46 EC (the "Data Protection Directive"), but there is a difficulty in anticipating compliance with such derogations & special conditions because they will depend on how Member States introduce, or retain, laws and rules in this area.

Commentary

Special cases

The GDPR contains broad derogations and exemptions in two main areas: (1) in Chapter III Section 5, regarding *"restrictions"* to obligations and data protection rights; and (2) in Chapter IX, regarding *"specific processing situations"*.

Article 23 - Restrictions

Article 23 of the GDPR creates the right for Member States to introduce derogations to data protection law in certain situations; this is also the case in the Data Protection Directive. Member States can introduce derogations from transparency obligations and data subject rights, but only where the measure *"respects the essence of … fundamental rights and freedoms and is … necessary and proportionate … in a democratic society"*.

The measure must safeguard one of the following:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences or breaches of ethics in regulated professions;
- other important public interests, in particular economic or financial interests (e.g. budgetary and taxation matters);
- the protection of judicial independence and proceedings;
- the exercise of official authority in monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the data subject, or the rights and freedoms of others; or
- the enforcement of civil law matters.

In order for a measure to be acceptable, it must (in accordance with Article 23(2)) include specific provisions setting out:

- the purposes of processing;
- the affected categories of data;
- the scope of the restrictions to the GDPR which are introduced by the measure;
- safeguards to prevent abuse, unlawful access or transfer;
- the controllers who may rely on the restrictions;
- the applicable retention periods and security measures;
- the risk to data subjects' rights and freedoms; and
- the right of data subjects to be informed about the restriction, unless this is prejudicial to the purpose of the restriction.

Articles 85-91: "Specific Data Processing Situations"

The provisions in Chapter IX GDPR provide for a mixed set of derogations, exemptions and powers to impose additional requirements, in respect of GDPR obligations and rights, for particular types of processing. These different provisions build upon specific processing situations already handled by the Data Protection Directive.

Article 85: Freedom of expression and information

This provision effectively repeats a Member State obligation under the Data Protection Directive and earlier data protection instruments to introduce exemptions to the GDPR where necessary to *"reconcile the right to the protection of personal data…with the right to freedom of expression and information."* This specifically applies to processing carried out for journalistic purposes, or for the purposes of academic, artistic or literary expression. Member States will be required to notify the Commission on how they have implemented this requirement and of any changes to such laws.

Article 86: Public access to official documents

This provision expands on Recital 72 of the Data Protection Directive, and allows personal data within official documents to be disclosed in accordance with Union or Member State laws which allow public access to official documents. This is not without limit - such laws should, according to Recital 154 GDPR, *"reconcile public access to official documents…with the right to protection of personal data"*. Directive 2003/98/EC (the "PSI Directive") on the *"re-use of public sector information"* does not alter the obligations on authorities, or rights of individuals, under the GDPR.

Article 87: National identification numbers

This effectively replicates the right of Member States to set their own conditions for processing national identification numbers under the Data Protection Directive. The only expansion is to clarify that this requires appropriate safeguards to be put in place.

Article 88: Employee data

Member States are permitted to establish (either by law or through collective agreements) more specific rules in respect of the processing of employee personal data, covering every major aspect of the employment cycle from recruitment to termination. This includes the ability to implement rules setting out when consent may be deemed valid in an employment relationship. Such rules must include specific measures to safeguard the data subject's *"dignity, legitimate interests and fundamental rights"* and the GDPR cites the transparency of processing, intragroup transfers and monitoring systems as areas where specific regard for these issues is required. Member States must notify the Commission of any laws introduced under this Article by the time the GDPR enters into force, and must also notify it of any amendments.

Article 89(1) and (2): Scientific and historical research purposes or statistical purposes

Article 89(1) acknowledges that controllers may process data for these purposes where appropriate safeguards are in place (see section on lawfulness of processing and further processing and sensitive data and lawful processing). Where possible, controllers are required to fulfil these purposes with data which does not permit, or no longer permits, the identification of data subjects; if anonymisation is not possible, pseudonymisation should be used, unless this would also prejudice the purpose of the research or statistical process.

Article 89(2) allows Member States and the EU to further legislate to provide derogations from data subject rights to access, rectification, erasure, restriction and objection (subject to safeguards as set out in Article 89(1)) where such rights *"render impossible or seriously impair"* the achievement of these specific purposes, and derogation is necessary to meet those requirements.

The recitals add further detail on how *"scientific research"*, *"historical research"* and *"statistical purposes"* should be interpreted. Recital 159 states that scientific research should be *"interpreted in a broad manner"* and includes privately funded research, as well as studies carried out in the public interest. In order for processing to be considered statistical in nature, Recital 162 says that the result of processing should not be *"personal data, but aggregate data"* and should not be used to support measures or decisions regarding a particular individual.

Article 89(1) and (3): Archiving in the public interest

The same derogations and safeguards exist for *"archiving in the public interest"* as are mentioned above in respect of processing for research and statistical purposes, except that derogations may also be granted for the right to data portability. Further detail is included in Recital 158, which suggests that this should only be relied upon by bodies or authorities that have an obligation to interact with records of *"enduring value for general public interest"* under Member State or Union law.

Article 90: Obligations of secrecy

This Article allows Member States to introduce specific rules to safeguard *"professional"* or *"equivalent secrecy obligations"* where supervisory authorities are empowered to have access to personal data or premises. These rules must *"reconcile the right to protection of personal data against the obligations of secrecy"*, and can only apply to data received or obtained under such obligation. Again, Member States must notify the Commission of any laws introduced under this Article by the time the GDPR enters into force, and must also notify it of any amendments.

Article 91: Churches and religious associations

This Article protects *"comprehensive"* existing rules for churches, religious associations and communities where these are brought into line with the GDPR's provisions. Such entities will still be required to submit to the control of an independent supervisory authority under the conditions of Chapter VI (see section on co-operation and consistency between supervisory authorities).

Where can I find this?

Derogations
Article 23, Recital 73

Special conditions
Articles 6(2), 6(3), 9(2)(a), 85-91
Recitals 50, 53, 153-165

Delegated acts, implementing acts and final provisions

At a glance

The final chapters of the GDPR provide confirmation of when the GDPR will come into force (likely to be summer 2018) together with its intended relationship with other EU data protection instruments including Directive 2002/58/EC (the "e-Privacy Directive").

The Commission will report regularly on the GDPR once it comes into effect. These final provisions also give the power to the Commission to adopt certain delegated acts under the GDPR (i.e. in respect of the use of icons and certification mechanisms).

To do list

- ☐ Note the date that the GDPR will come into force.
- ☐ Start planning what changes you will need to make to address the new requirements. See action points from other sections.
- ☐ Where relevant to your business, look out for further developments in connection with the e-Privacy Directive. A consultation is imminent.

Commentary

Chapter 10 of the GDPR grants the Commission the power to adopt delegated acts (as referred to in Article 12(8) in respect of standardised icons and in Article 43(8) in respect of certification mechanisms). These powers can be revoked by the Parliament or the Council at any time. The acts adopted will enter into force within 3 months, provided neither the Parliament nor the Council objects. This period can be extended. The Commission will be assisted by a committee, in accordance with Regulation 182/2011. It is of particular importance that the Commission carry out appropriate consultations when carrying out its preparatory work, including at expert level (Recital 166).

Implementing powers are also conferred on the Commission in order to ensure uniform conditions for the implementation of the GDPR which should also be exercised in accordance with Regulation 182/2011.

Chapter 11 of the GDPR confirms that the Data Protection Directive will be repealed once the GDPR comes into effect which will be two years and twenty days following its publication in the Official Journal (likely to be spring 2018) and that references to the repealed Data Protection Directive shall be construed as references to the GDPR.

The Commission will report regularly on the GDPR to the Parliament and the Council, with particular focus on the data transfer provisions and the co-operation and consistency provisions. The first report shall be made no later than 4 years after the GDPR comes into force and will be submitted every 4 years thereafter. The reports will be made public.

The GDPR does not impose additional obligations on persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective as set out in the e-Privacy Directive (Article 95). However, the Commission commits to reviewing other EU data protection instruments and in particular, the e-Privacy Directive (Recital 173) in order to ensure consistency with the GDPR.

Recital 171 clarifies that where processing is based on consent under the current Data Protection Directive, it is not necessary for the individual to give their consent again if the way the consent has been given is in line with the conditions of the GDPR.

Where can I find this?

Articles 92-99, Recitals 166-173

Glossary

Data controller
A person or body, alone or jointly, which determines the purposes and means of processing personal data.

Data processor
An entity which processes the data on behalf of the data controller.

Data Protection Directive
The European Directive 95/46/EC previously governed the processing of personal data in the EU and will now be replaced by the GDPR.

DPO
Where: (i) processing is carried out by a public authority; or (ii) processing consists of "the systematic monitoring of data subjects on a large scale" or; (iii) the "core activities" of the data controller and data processor consist of the processing "on a large scale of special categories of data" there is an obligation to designate a Data Protection Officer who will inform and advise on data protection matters, monitor compliance and cooperate with, and act as a point of contact for, the supervisory authority.

EDPB
The European Data Protection Board; it will replace the Article 29 Working Party and its functions will include ensuring consistency in the application of the GDPR, advising the EU Commission, issuing guidelines, codes of practice and recommendations, accrediting certification bodies and issuing opinions on draft decisions of supervisory authorities.

EEA
The European Economic Area includes all 28 EU member states, plus Iceland, Lichtenstein and Norway. It does not include Switzerland.

Personal data
This is any information relating to an identified/ identifiable, natural person, a 'data subject'. A data subject is a natural person, who can be identified, or is identifiable, directly or indirectly.

PIA
The GDPR imposes a new obligation on data controllers and data processors to conduct a Data Protection Impact Assessment (otherwise known as a privacy impact assessment, or PIA) before undertaking any processing that presents a specific privacy risk by virtue of its nature, scope or purposes. Chapter IV Section 3 sets out a non-exhaustive list of categories of processing that will fall within this provision.

Process
This is defined widely to cover any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means. Examples of processing include the collection, recording, organisation, storage, use and destruction of personal data.

Pseudonymisation
The technique of processing personal data so that it can no longer be attributed to a specific individual without the use of additional information, which must be kept separately and be subject to technical and organisational measures to ensure non-attribution.

Right to erasure / right to be forgotten
The data subject's existing right to deletion of their personal data, in certain circumstances, has been extended to a new 'right of erasure' in circumstances detailed in Chapter III Section 3 GDPR.

Special categories of data
Often known as 'sensitive data'. The GDPR has extended the definition to include both biometric and genetic data.

Subject access
This is the data subject's right to obtain from the data controller, on request, certain information relating to the processing of his/ her personal data as detailed in Chapter III Section 2 GDPR.

Supervisory authority/lead authority
Supervisory authorities are national data protection authorities, empowered to enforce the GDPR in their own member state.

The 'one-stop-shop' concept: 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. A supervisory authority which is not a lead authority may also have a regulatory role, for example where processing impacts on data subjects in the country where that supervisory authority is the national authority.

Transfer
The transfer of personal data to countries outside the EEA or to international organisations, which is subject to restrictions detailed in Chapter V GDPR. As with the Data Protection Directive, data does not need to be physically transported to be transferred. Viewing data hosted in another location would amount to a transfer for GDPR purposes.

An undertaking
This term is used in a variety of contexts in the GDPR, most often to refer to a legal entity that is engaged in "economic activity". The term has a particular meaning in the context of the GDPR's provisions regarding financial penalties. Undertakings will be subject to penalties calculated as a percentage of their annual world wide turnover. In this context, the term imports principles developed in the context of EU competition law.

Practice Co-heads

Ruth Boardman
Partner
+44 (0)20 7415 6018
ruth.boardman@twobirds.com

Ariane Mole
Partner
+33 (0)1 42 68 6304
ariane.mole@twobirds.com

Experts in every office

twobirds.com

Aarhus & Abu Dhabi & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Düsseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Stockholm & Sydney & Warsaw