MASON HAYES & CURRAN

Getting Ready for the General Data Protection Regulation

Dublin, London, New York & San Francisco

A Guide by Mason Hayes & Curran

MHC.ie

Table of contents

1. What is the GDPR?

*The EU General Data Protection Regulation (EU) 2016/679 ('**GDPR**'), which comes into force on 25 May 2018, marks a significant change in the EU data protection regime. The GDPR will repeal and replace the current Data Protection Directive, Directive 95/46/EC (the 'Directive'), which forms the basis for the existing data protection regime.*

The GDPR was first published as a draft proposal in January 2012 and, after a long legislative process, was adopted on 27 April 2016. Upon its coming into force on 25 May 2018, many of the GDPR's significant changes will take effect. Some of its more innovative provisions will take more time since they require additional codes and guidance to be developed and approved.

As a Regulation, and unlike the preceding Directive, the GDPR will be immediately enforceable in Ireland (and the other EU Member States) without the need for domestic implementing legislation. This should reduce the level of national variation in relation to data protection law across the EU. It also recognises the so-called 'one-stop-shop' which enables organisations with pan-European operations to benefit from primary regulation by a single national supervisory authority in just one EU state. This increased level of harmonisation of laws across the EU and recognition of the one-stop-shop should make it easier for businesses that sell goods or services across the EU to take a more unified approach to data protection compliance. However, complete EU-wide uniformity will not consequentially occur as the GDPR has left discretion to Member States in a number of areas. Additionally, running to over 88 pages, the GDPR is not without complexity leading to the consequent risk of differing national interpretations.

The GDPR builds upon familiar concepts and rules in the Directive, which is welcomed. However, in many respects it extends considerably further than the Directive. It has wider scope, standards have been raised, and sanctions are higher; up to the greater of 4% of annual revenue or €20 million.

In particular, the introduction of the 'accountability principle' means that affected organisations will have to work on their internal compliance, including record keeping and, for some, the appointment of a data protection officer.

The GDPR expands the territorial scope of EU data protection law, and applies both to organisations established in the EU and to non–EU established organisations that target or monitor EU residents. A wider number of organisations will now be captured by EU data protection law.

New requirements relating to consent, breach notification, transparency, accountability and the appointment of data protection officers, are introduced. This means all impacted organisations will need to revise both their policies and operational procedures. Changes are especially important due to significant penalties and fines for non-compliance.

Sanctions increase:
Up to 4% of annual revenue or €20 million

The changes brought about by the GDPR, particularly the increased compliance burden and higher sanctions, emphasise the need for organisations to review and enhance their existing practices, policies and record-keeping, especially as organisations will need to be able to demonstrate compliance when called upon to do so.

Businesses have some time before the GDPR comes into effect. However, getting to grips with a new compliance framework takes time, particularly given the likely impact of the GDPR on practical day-to-day operations. Organisations should accordingly start preparing for the GDPR now if they have not already started doing so.

2. Executive summary

Does the GDPR Apply to Me?

Section 3 investigates the scope of application for the GDPR. Some controllers and processors who fall outside the Directive will now be subject to the GDPR.

- Territorial Scope: The GDPR applies if an entity is established in the EU, and is engaged in the processing of personal data in the context of that establishment's activity, even if the processing itself takes place outside the EU. The GDPR also applies to entities without an establishment in the EU if they process personal data of EU data subjects, and the data relates to goods or services offered to EU data subjects or the monitoring of behaviour in the EU.

- Material Scope: The GDPR applies to the electronic or automated processing of personal data and to manual paper-based processing if the personal data forms part of, or is intended to form part of, a filing system.

How Can I Prepare for the Implementation of the GDPR?

In Section 4 we provide a roadmap to 5 key steps that organisations should take in preparation for the GDPR: Gap and Compliance Analysis; Contracting and Policies; Record-Keeping and Privacy Governance; Security; and 'Privacy Impact Assessment' and 'Privacy by Design'.

How Does the GDPR Alter Current Data Protection Law?

In Section 5 we identify the GDPR's most significant changes to data protection law. These are:

- The GDPR refines the definitions of personal data and sensitive data. Personal data now extends to online identifiers such as IP addresses and cookies. The definition of sensitive personal data is expanded to include genetic and biometric data.

- The GDPR contains a tougher 'data minimisation' principle than the Directive. It also introduces a new 'accountability' principle.

- The GDPR tightens the rules on how consent is obtained. Consent must be freely given, specific, informed and provided via an unambiguous indication of the data subject's wishes. The requirement that some type of affirmative action is required for valid consent is a significant change. The onus of proving that proper consent was obtained lies with the data controller. Consent may not be rolled in with other contractual terms, and the data subject retains the right to withdraw that consent at any time. If the performance of a contract is conditional on consent to the processing of personal data, strict criteria apply before the consent will be treated as voluntary.

- The GDPR introduces novel rules for the processing of children's data. These rules govern online consents, privacy notices and the justification of processing by reference to the legitimate interests of the controller or third party, if the data subject is a child.

- The GDPR establishes new rights for data subjects and corresponding duties for controllers and processors. The rights of rectification and erasure are strengthened, while data subjects gain a right to restriction of processing. A right of data portability gives data subjects the right to receive personal data and to transmit that data to another controller. Controllers have new obligations to notify third party recipients of information of requests for rectification, restriction or erasure.

- The GDPR establishes new requirements for the contents of privacy notices.

- 'Privacy by Design' and 'Privacy by Default' are important new concepts under the GDPR. Privacy by Design requires organisations to consider privacy measures during product design processes, while Privacy by Default requires controllers to ensure that, by default, only necessary data is processed.

- The GDPR mandates the appointment of a Data Protection Officer in certain instances which will introduce new compliance costs for organisations.

- The GDPR contains new security requirements, such as new rules on data breaches.

- The GDPR implements a new regime for enforcement, remedies and liability. Under the 'one-stop-shop,' the lead regulator for controllers and processors engaged in cross-border processing is the supervisory authority in the Member State where they have their main establishment. However, complaints can be made to any supervisory authority, and in some cases, another supervisory authority may carry out an investigation. The GDPR establishes new rules on compensation for infringement, which extend to both material and non-material damage, and provides for the imposition of significant administrative fines by the national supervisory authority.

- Finally, the GDPR encourages the drawing up of codes of conduct and the development of data protection certification mechanisms.

What does the GDPR mean for ... ?

In Section 6 we trace the impact of the GDPR on certain commercial activities. In contracting, the GDPR increases the importance of carefully drafted clauses on data export, engagement of joint controllers, processors and sub-processors, and the apportionment of liability. In compliance and risk management, the accountability principle means that controllers and processors bear the burden of demonstrating that they comply with the GDPR. Human resource managers should be aware that the GDPR allows Member States to adopt more specific rules for data processing in the employment context, and revises the law on subject access requests. Technology-driven businesses should note the new, more stringent rules on user consent, and on the enhanced rights of data subjects. In disputes/litigation, the GDPR's key changes relate to jurisdiction and the role of the supervisory authority.

3. Does the GDPR apply to me?

The GDPR applies to all entities established in the EU which process personal data, regardless of whether the processing takes place in the EU. It also applies to a wide range of entities established outside the EU, where they collect or process personal data relating to EU residents. This means a number of controllers and processors which currently fall outside the Directive will now be subject to EU data protection law.

3.1 Territorial scope

By applying to controllers and processors within the EU, as well as certain controllers and processors outside the EU, the GDPR significantly extends the territorial scope of EU data protection law. We consider how both EU-established and non-EU established entities can be affected.

A. EU established

The GDPR applies to controllers and processors who have an EU establishment and who are engaged in the processing of personal data in the context of that establishment's activity. This is the same test that currently applies under the Directive.

There is no requirement that the actual data processing occur within the EU. In other words, using servers outside the EU will not bring an EU company outside of the scope of the GDPR.

To address situations where a controller or processor has more than one establishment in the EU (e.g. offices in a number of Member States), the GDPR recognises the so-called 'one-stop-shop' through the concept of a 'main establishment', with a single 'lead supervisory authority'.

What constitutes an EU establishment?

The GDPR states that an establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements is not itself the determining factor.

- The Court of Justice of the European Union ('CJEU') has considered the term 'establishment' within the context of the Directive in *Google Spain SL, Google Inc. v AEPD (C-131/12), Weltimmo (C-230/14)* and more recently in *VKI v Amazon EU Sárl (C-191/15)*. These cases continue to be relevant under the GDPR. In *Google Spain*, the CJEU held that EU based sales and advertising operations carried out by a subsidiary of a US company constituted an establishment of that US company within the EU.

- In *Weltimmo*, the CJEU held that an establishment does not exist in a Member State merely because an undertaking's website is accessible there.

- In *VKI v Amazon EU Sárl*, the CJEU held that it is for the national court of the relevant Member State to decide whether data processing was carried out in the context of an establishment situated in a Member State.

B. Non-EU established entities offering goods or services within the EU or monitoring EU data subjects

The GDPR also applies to controllers and processors without an establishment in the EU where they process personal data of data subjects and that data relates to:

- Offering of goods or services to data subjects within the EU, regardless of whether a payment is required, or
- Monitoring of the behaviour of data subjects within the EU.

C. Non-EU established controllers where EU law applies by virtue of public international law

As under the Directive, the GDPR applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law, such as in a Member State's diplomatic mission or consular post. Practically speaking, the circumstances in which the laws of a Member State apply by virtue of public international law tend to be very limited. For example, the management of human resource data in a Member State embassy outside the EU might be captured under this rule.

When is an entity offering goods or services to data subjects in the EU?

The test is whether the controller 'envisages' offering goods or services to data subjects in the EU, and a number of factors are relevant:

- This test is not met simply by the mere accessibility of a website in the EU
- A number of factors may suggest that a controller envisages offering goods or services to data subjects in the EU, including:
  - using a language or currency generally used in one or more Member States, or
  - mentioning customers or users who are in the EU
- It does not matter whether the good or service is provided with or without charge.

When is an entity monitoring the behaviour of data subjects within the EU?

- The application of the GDPR to non-EU established controllers and processors in these instances is a significant extension in the territorial scope of EU data protection law. The Directive currently requires compliance by non-EU established controllers only where controllers make use of equipment situated within the EU.
- In order to determine whether a processing activity monitors the behaviour of data subjects, you need to look at things like whether individuals are tracked on the internet, or are subject to data processing techniques like profiling and predictive and other analysis regarding personal preferences, behaviours and attitudes.

CASE STUDY

Red Inc., an e-commerce retailer, is incorporated in Canada with its headquarters in Vancouver, Canada. It has no offices, personnel or physical presence within the EU. It sells goods to EU residents via its website, in its customers' local languages and currencies, and offers delivery rates to EU countries. While Red Inc. may not necessarily have been subject to EU data protection law under the Directive, it will be subject to the GDPR.

Red Inc. will also have to appoint a representative in the EU who will act as a point of contact for supervisory authorities.

3.2 Material scope

Like the Directive, the GDPR applies to the processing of personal data wholly or partly by automated means (such as a computerised system) and to manual processing if the personal data form part of a filing system or are intended to form part of a filing system.

As under the Directive, certain forms of processing fall outside the scope of the GDPR. The GDPR is not applicable to the processing of personal data:

- By a natural person in the course of a purely personal or household activity (the '**household exemption**')
- Concerning the personal data of deceased persons
- By competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of threats to public security
- By EU institutions where a unique Regulation for processing personal data by EU institutions will continue to apply instead of the GDPR
- In the course of an activity which falls outside the scope of EU law (e.g. activities concerning national security), or
- Relating to the EU's common foreign and security policy

The household exemption: This exemption includes correspondence and the holding of addresses, or social networking and online activity undertaken for those purposes. For example, having a personal address book will not be captured by EU data protection law.

- In *Ryneš (C-212/13)*, the CJEU held that activities that are only partly personal, for example, sending correspondence that includes both personal and professional content, do not fall within the household exception.

- The GDPR is, however, applicable to controllers or processors that provide the means for processing personal data for personal or household activities, such as email service providers.

KEY TERMS AND WHERE TO FIND THEM

Establishment – Recital 22: Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

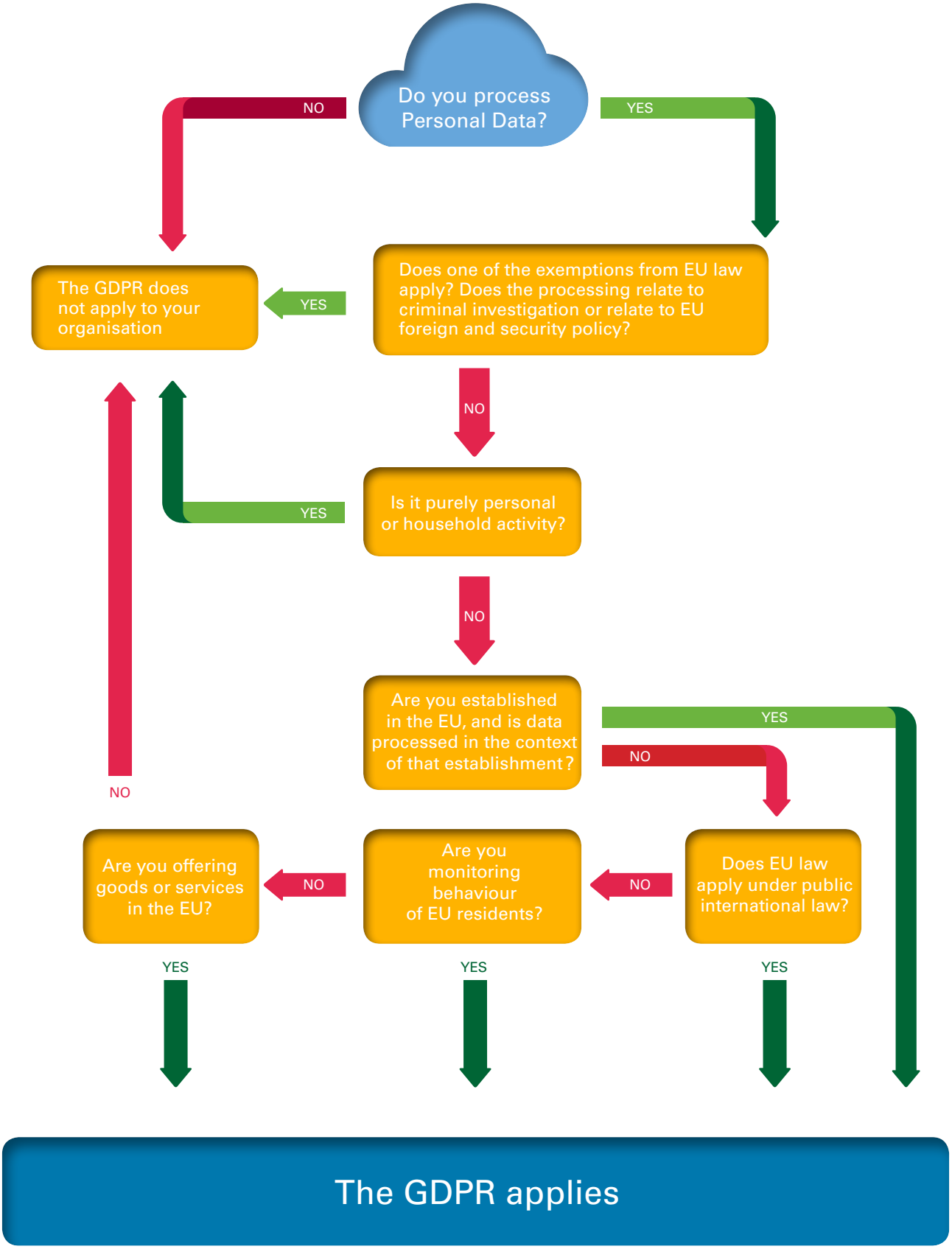
Filing System – Article 4(6): Any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Material Scope – Article 2, Recitals 15 – 19: the types of activities regulated by the GDPR. *See also* Recital 27.

Processing – Article 4(2): Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Territorial Scope – Article 3: the level of connection to the EU necessary to be captured by the GDPR. *See also* Recitals 23 – 25.

Does the GDPR apply to my organisation?



4. How can I prepare for the implementation of the GDPR?

The checklist highlights 5 key steps that organisations should consider to help in their preparation for the GDPR.

1. GAP AND COMPLIANCE ANALYSIS

- Review of products and services
- Review data sets and management (including data capture, disclosures to third parties and data exports to outside the European Economic Area)
- Review of current privacy notices and policies (including method for communicating to relevant individuals and, if applicable, capturing consent)
- Review current suite of privacy compliance documentation
- Review current legal bases relied upon for processing personal data
- Review any uses of children's data or sensitive personal data
- Identify gaps in your compliance with current EU law and the GDPR and identify compliance actions

2. CONTRACTING AND POLICIES

- Identify third party contracts related to personal data
- Develop templates for:
  - Data processing agreements for third party service providers
  - Intra-group data processing agreements (where relevant)
  - Joint control contracts
  - Liability apportionment clauses
  - Intra-group data export agreements (where relevant)
- Update public and employee privacy notices and policies
- Review terms and conditions which capture privacy consents

3. GOVERNANCE

- Develop accountability programme and review process
- Draft or amend suite of compliance documentation, including data breach register, data governance records and privacy impact assessments
- Select and appoint Data Protection Officer (where relevant)
- Update subject access request handling policy
- Update personnel training on data protection
- Develop organisational compliance methodology

4. SECURITY

- Review security protocols, and consider integration of security measures specified under the GDPR including encryption and pseudonymisation
- Familiarise yourself with the notification obligations for security breaches under the GDPR
- Draft template security breach notifications and security breach response plan

5. PRIVACY IMPACT ASSESSMENT AND PRIVACY BY DESIGN

- Draft privacy impact assessment questionnaire
- Develop privacy impact assessment and privacy by design implementation and review process

5. How does the GDPR alter current data protection law?

The GDPR extends a number of familiar concepts and rules in the Directive. The key changes made by the GDPR to EU data protection law are described in this section.

5.1 Definitions of personal and sensitive data

The GDPR extends the definitions of both personal data and sensitive personal data.

A. Personal data

As under the Directive, personal data is any information relating to an identified or identifiable natural person. The GDPR has expressly added name, location data, online identifiers and factors specific to the genetic identity of a natural person to the list of factors by which a natural person may be identified. Under the Directive, the definition of personal data was less specific, though the general view was that such identifiers were usually already captured (particularly in light of *Breyer (C-582/14)*.

The inclusion of online identifiers is notable. It will result in IP addresses and cookies, where they can lead to the identification or singling out of individuals, falling within the scope of the GDPR.

In practical terms, the modified definition of personal data is unlikely to result in significant change owing to the broad definition of personal data endorsed by the CJEU in *Breyer (C-582/14)*. In *Breyer*, the Court held that a dynamic IP address can constitute personal data. In more general terms, the Court held that where an organisation holds data that alone cannot identify an individual, that data may constitute personal data if the organisation has the legal means which enable it to identify the data subject by combining the data with other information held by one or more third parties.

A related concept of 'pseudonymisation' is introduced for the first time by the GDPR. Pseudonymisation concerns the processing of personal data in such a way so as to prevent an individual being directly or indirectly identified from that data without the use of additional information. Provided that the additional information is kept separate and secure, the risks associated with pseudonymous data are likely to be lower. Pseudonymous data is still treated as personal data because it enables the identification of individuals. However, use of pseudonymous data may justify processing that would otherwise be deemed 'incompatible' with the purposes for which the data was originally collected, and can be adopted as a helpful security or privacy by design measure.

B. Sensitive personal data

The definition of special categories of data, i.e. sensitive personal data or sensitive data, is extended by the GDPR, adding genetic and biometric data to this protected category of data.

Under this expanded definition, the specially protected categories of data extend to processing of:

- Data revealing:
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs, or
  - Trade union membership
- Genetic data or biometric data for the purpose of uniquely identifying a natural person, or
- Data concerning health, a natural person's sex life, or sexual orientation

As under the Directive, more onerous conditions must be satisfied in order to legitimise the processing of sensitive data. Sensitive data may be processed where the data subject gives his or her explicit consent to such processing, or where a specific derogation is in place. The derogations include:

- Necessary processing in the fields of employment, social security and social protection where authorised by law or collective agreement
- Processing to protect the vital interests of the data subject or another natural person where the data subject is incapable of giving consent
- Processing by certain non-profit organisations
- Processing of personal data which are manifestly made public by the data subject
- Processing in relation to legal claims or by courts acting in their judicial capacity
- Processing necessary for reasons of substantial public interest, on the basis of compatible and proportionate law
- Processing for the purposes of preventative occupational medicine
- Processing for reasons of public interest in the area of public health, and
- Processing necessary for scientific or historical research

Biometric data and photographs

- *The processing of photographs will not automatically be considered as the processing of biometric data. However, photographs will be covered where they allow the unique identification or authentication of an individual as a biometric, for example, where they are used as part of an electronic passport or for the purposes of facial recognition.*

Notably, Member States are entitled to maintain or impose further conditions in respect of genetic, biometric or health data. Consequently, national variations are likely to persist.

CASE STUDY

Magenta Unlimited Company provides a software app which, among other things, records a user's heart rate using the camera of a smartphone. This amounts to the processing of data relating to a user's health and, accordingly, requires that user's explicit consent.

Cyan Ltd is a clothes retailer which requires its employees to submit medical certificates in order to certify absences from work of more than two days. As this is necessary for employment reasons, and authorised by the law of the Member State in which Cyan is established, this is acceptable under the GDPR.

C. Data concerning criminal convictions

The GDPR does not make any material changes in respect of the processing of data concerning criminal convictions, offences and related security measures. As under the Directive, this category of data is not sensitive data but nonetheless the processing of this category of data is subject to specific protection. Processing may only be carried out under the control of national authorities. National law may provide exceptions to this rule, subject to suitable safeguards. Existing Irish law has dealt with criminal record information requirements by including it within the definition of sensitive personal data.

KEY TERMS AND WHERE TO FIND THEM

Biometric data – Article 4(14): Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprint information. *See also* Recitals 51, 53, 91.

Data concerning health – Article 4(15): Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
See also Recitals 35, 53 – 54.

Data concerning criminal convictions – Article 10. *See also* Recitals 19, 50, 73, 80, 91, 97.

Genetic data – Article 4(13): Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
See also Recitals 34 – 35, 53, 75.

Personal data – Article 4(1): Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Pseudonymisation – Article 4(5): The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.
See also Articles 6(4)(e), 25(1), 32(1)(a), 40(2)(d), 89(1) and Recitals 26, 28 – 29, 75, 78, 156.

Sensitive data – Article 9: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. *See also* Recitals 10, 34, 35, 51.

5.2 Data protection principles

The data protection principles are the fundamental principles relating to how personal data may be processed. The principles in the GDPR are in broadly similar terms to those contained in the Directive, with some additions, most notably the introduction of the accountability principle. The principles are as follows:

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and transparently. Organisations should read this transparency requirement in light of the requirement to provide more detailed privacy notices to data subjects.

Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes. It cannot be further processed in a manner incompatible with those purposes.

Exceptions: Further processing of personal data for scientific and historical research purposes or statistical purposes will not be considered incompatible with the original processing purposes. The GDPR adds that further processing of personal data for archiving purposes in the public interest will not be considered incompatible with the original processing purposes. Further processing is subject to the implementation of appropriate technical and organisational measures.

Data minimisation

Personal data must be adequate and relevant, under both the Directive and the GDPR. However, this standard appears to be tougher under the GDPR. The Directive's obligation to ensure that personal data is 'not excessive' is replaced by a requirement to ensure that personal data is 'limited to what is necessary'. Organisations may have to review their data processing operations in order to ascertain whether they process any personal data which is unnecessary having regard to the relevant purpose for which processing is carried out.

Accuracy

Personal data must be accurate, and where necessary kept up to date. Reasonable steps must be taken to ensure that inaccurate personal data is erased or rectified without delay.

Storage limitation

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary.

Exceptions: Personal data may be stored for longer periods for scientific or historical research purposes or statistical purposes, or archiving purposes in the public interest, provided appropriate technical and organisational measures are implemented.

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. While this requirement existed under the Directive, the GDPR now specifically categorises it as a data protection principle.

Accountability

Accountability is a new concept introduced by the GDPR. It requires controllers to be able to demonstrate how they comply with the data protection principles listed. This is significant as it shifts the burden of proof to the data controller in the event of a compliance investigation by a data protection authority. Organisations should view this principle in light of the record keeping obligation, the requirement to prove that consent is obtained and the concept of privacy by design and default.

KEY TERMS AND WHERE TO FIND THEM

Data Protection Principles - Article 5. *See also* Recitals 29, 39, 50, 71, 85, 156.

5.3 Valid consent

A lawful basis is required for the processing of personal data. The grounds for lawful processing in the GDPR replicate those in the Directive. One of the lawful grounds for processing is the consent of the data subject.

The GDPR tightens the concept of consent. Accordingly, obtaining the consent of a data subject will be more difficult under the GDPR. In particular, this is due to the requirement of separate consents for different processing operations, the prohibition on including consent in the terms of service, and the data subject's express right to withdraw his or her consent at any time.

- **FREELY GIVEN**
- **SPECIFIC**
- **INFORMED**
- **UNAMBIGUOUS**

Under the GDPR, in order to provide a lawful basis for processing, the consent of a data subject must be:

1. **Freely given** – Consent will not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

2. **Specific** – When the processing has multiple purposes, consent should be obtained for each of them.

3. **Informed** – For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data is intended. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

4. **An unambiguous indication of the data subject's wishes by a statement or clear affirmative action** – Clear affirmative actions which may provide evidence of consent include ticking a box when on a webpage, choosing technical settings on a website, or 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 will not suffice.

- **ONUS OF PROOF**
- **INDEPENDENT CLAUSE**
- **RIGHT OF WITHDRAWL**
- **VOLUNTARY**

In order for consent to be valid, four additional criteria must be complied with:

1. **Onus of proof:** The controller must be able to demonstrate that the data subject has consented to the processing of his or her personal data. Consequently, a record should be maintained evidencing a data subject's consent.

2. **Independent consent clauses:** Where consent is provided in a written declaration, such as a contract, that contains additional matters, the request for consent must be clearly distinguishable from other matters in that declaration. It must further be intelligible, easily accessible and be in clear and plain language. A consent clause contained in the middle of a set of general terms and conditions is unlikely to suffice.

3. **Right of withdrawal:** The data subject is entitled to withdraw his or her consent at any time and must be informed of the existence of this right. It must be as easy to withdraw as it is to give consent.

4. **Voluntary:** When assessing whether consent is freely given, utmost account must be taken of whether the performance of a contract is conditional on a data subject consenting to the processing of personal data that is not necessary for the performance of that contract. Consent in such instances is unlikely to be regarded as freely given.

There is no change in the law in respect of the requirement of explicit consent for the processing of sensitive data. Similar to the Directive, no definition of explicit consent is provided in the GDPR.

In some instances it may be permissible to rely on existing consents secured under the Directive.

It is not necessary for the data subject to give his or her consent again if the way the consent given under the Directive is in line with the conditions of the GDPR.

In such cases, the data controller may continue processing on the basis of consent given prior to the date the GDPR takes force. However, in many cases, historic consents may not be compliant with the requirements of the GDPR. Data controllers will accordingly need to review historic consents to determine their compliance with the GDPR.

KEY TERMS AND WHERE TO FIND THEM

Consent - Article 5. Article 4(11): Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
See also Articles 6(1), 7 and Recitals 32, 40, 42, 43, 65, 171.

CASE STUDY

Turquoise plc is a bank. When its customers sign up for new accounts, it requires them to sign the following consent form, without providing a data protection notice:

'All customers who sign up for accounts consent to the use of their personal data in perpetuity, for whatever purposes Turquoise plc sees fit.'

Turquoise plc has failed to obtain a valid consent – the consent is not informed as an explanation of the specific purposes for which the data may be used was not provided. This consent form also makes the service, in this case the provision of a bank account, conditional on consent to unspecified uses and those uses may not be necessary to provide that service. This is prohibited by the GDPR. A valid consent also comes with a right of withdrawal and the reference to the consent extending 'in perpetuity' could be seen to imply that there is no such right.

5.4 Children's data

The GDPR introduces a number of specific requirements relating to the processing of children's data.

Online consents

- Where information society services, such as online services, are offered directly to a child under the age of 16 and the child is required to consent to the processing of his or her personal data, parental consent must be obtained. However, Member States may specify an age limit below 16 years provided that the age restriction does not fall below 13 years.

- The controller is required to make 'reasonable efforts' to verify that consent has been given or authorised by the parent/guardian of the child, bearing in mind available technology. This means specific verification measures should be used.

- Specific protections must be applied to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

- The introduction of this age limit will not affect contract law rules on the validity, formation or effect of a contract in relation to a child.

Privacy notices

- Controllers are required to take appropriate steps to ensure that the provision of information to data subjects is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is especially important in respect of information addressed specifically to a child. Where processing is addressed to a child, any information and communication should be in such a clear and plain language that the child can easily understand.

Legitimate interests

- The pursuit of legitimate interests by the controller or a third party is a basis for lawful processing instead of consent. Relying on this basis involves a balancing test between the competing interests involved. The interests of the controller or third party may be overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. The protection of a child's interests as a data subject is particularly important.

5.5 Additional rights for data subjects

The GDPR provides data subjects with additional rights and protections, which equate to new obligations for controllers and processors. It also strengthens the concepts of rectification, erasure, restriction of processing that existed under, or were derived from, the Directive.

A. Rectification

A data subject is entitled to have inaccurate personal data concerning him or her rectified without undue delay. Data subjects are also entitled, taking into account the purposes of the processing, to have incomplete personal data completed.

KEY TERMS AND WHERE TO FIND THEM

Conditions applicable to children's consent – Article 8. See also Recital 38, 65.
Privacy Notices – Article 12(1), Article 13, Article 14. *See also* Recital 58, 71.
Legitimate Interests – Article 6(1)(f). *See also* Recital 47–50, 69.

B. Erasure

A data subject is entitled to have personal data concerning him or her erased in specified circumstances. This is known as the right of erasure or 'the right to be forgotten'. This entitlement is an extension of the right protected in the Directive. The Directive gave data subjects a right of erasure where their data was being processed in breach of the data protection principles, in particular because of the incomplete or inaccurate nature of the data. Importantly, this 'right to be forgotten' is distinct from the right of the same name set down by the CJEU in Google Spain, relating to delisting of search results.

Where the controller has made the personal data public and is subsequently obliged to erase the personal data, the controller may have further obligations. Taking account of available technology and the cost of implementation, the controller is required to take reasonable steps, including technical measures, to inform third party controllers who are processing the data, that the data subject has requested the erasure by such controllers of any links to, or copies of, those personal data.

When is there a right to erasure?

- The personal data is no longer necessary in relation to the purposes for which they were collected
- The data subject withdraws consent and there is no other legal ground for the processing
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing
- The personal data has been unlawfully processed
- The personal data has to be erased for compliance with a legal obligation under EU or Member State law, or
- The personal data has been collected in relation to the offer of information society services to a child

However, the right to erasure is not available where the processing of the relevant personal data is necessary:

- For exercising the right of freedom of expression and information
- For compliance with an EU or Member State legal obligation which requires processing by law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- For reasons of public interest in the area of public health;
- For certain archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- For the establishment, exercise or defence of legal claims

As the scope of the right to erasure is extended under the GDPR, organisations will be required to comply with a wider spectrum of erasure requests.

CASE STUDY

Pink GmbH runs an online dating website. Users register in order to create a profile, and respond to personality questionnaires to provide matches with other users.

Mr Lucky registered with the website, and, after a number of dates, entered into a long-term relationship and decided to close his account. Upon writing to Pink GmbH, Mr Lucky is entitled to have his personal data deleted as, after his account is closed and Mr Lucky withdraws his consent to the processing of his personal data, there is no continuing basis upon which Pink GmbH may continue to process his data.

C. Restriction of processing

The GDPR introduces a data subject's right to restrict processing. This right replaces the right to block certain uses as contained in the Directive.

There are four instances in which a data subject is entitled to restrict processing of his or her personal data as an alternative to erasure:

1. The accuracy of the personal data is contested by the data subject, in which case the processing is restricted for a period enabling the controller to verify the accuracy of the personal data

2. The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use instead

3. The controller no longer needs the personal data for the purposes of the processing, but the personal data is required by the data subject for the establishment, exercise or defence of legal claims, and

4. The data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject

When processing has been restricted, continued processing, with the exception of storage, may only occur in the following cases:

- The data subject consents
- The processing is necessary for the exercise or defence of legal claims
- The processing is necessary for the protection of the rights of other individuals or legal persons, or
- The processing is necessary for public interest reasons

A data subject is entitled to be notified by a controller before a restriction on processing is lifted.

D. Data portability

The GDPR introduces a new right of data portability which enables a data subject to receive personal data concerning him or her, in a structured, commonly used and machine-readable format, and to transmit that data to another controller without hindrance from the controller which provided the personal data. The right only applies to personal data that a data subject has provided to a controller.

The data subject may only exercise the right to data portability where the processing is based on the data subject's consent or is for the performance of a contract and the processing is carried out by automated means. The right to data portability will not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

WP29 Guidance:

The Article 29 Working Party ('WP29'), which comprises the European data protection authorities, has published a set of guidelines and frequently asked questions on the right to data portability which provide further detail as to extent of the obligations on controllers and processors.

WP29 guidance stresses that the right to portability is a right to both receive and transmit data from one service provider to another. WP29 encourages controllers to offer downloading options and a means to directly transmit the data to another data controller, for example by way of an application programming interface (or API). WP29 explains that while the receiving organisation will become the new data controller and must clarify its processing purposes with the data subject, the transmitting controller may still have obligations to the data subject, such as compliance with erasure or subject access requests.

WP29 considers the key limitation on the right of data portability, namely that the right extends only to data 'provided by the data subject'. WP29 takes an expansive view, suggesting two categories of data are provided by the data subject: (i) data actively and knowingly provided and (ii) observed data relating to the data subject's use of the service or device. Inferred data or derived data are not provided by the data subject and so fall outside of the scope of the right.

The distinction WP29 makes is that data which relate to the data subject's activity or result from the observation of an individual's behaviour are within the scope of the right, but that subsequent analysis of that behaviour is not.

CASE STUDY

Purple plc operates a music streaming service within which users can create playlists of their favourite music. In observing listening behaviour, Purple plc learns that particular users have preferences for particular artists or music albums and attributes traits to users to help personalise their experience and make relevant suggestions.

In order to comply with the right to data portability, Purple plc creates a tool which allows users to download their account information, and copies of their playlists, so they can switch to another service should they wish. Purple plc does not need to provide a copy of the traits it has attributed to User A as part of the right to data portability, although it may need to provide such information as part of the right of access.

E. Right to object to data processing

The Directive allowed a data subject to object to the processing of their data and the GDPR extends this right. The Directive permitted data subjects to object to the processing of their data on compelling legitimate grounds where the basis for that processing was either that the processing was in the public interest or in the legitimate interests of the controller and also in relation to processing for direct marketing.

While the GDPR similarly does not contain a general right to object, it lists certain instances in respect of which a data subject is given such a right:

- **Processing based on legitimate interest grounds or because it is necessary for a public interest task/ official authority:** This includes profiling based on these grounds. Following a data subject's objection to processing on either of these grounds, the controller is required to cease processing unless it demonstrates compelling legitimate grounds for the processing which override the rights of the data subject or the processing is necessary for the defence of legal claims.

- **Processing for direct marketing purposes:** Following an objection by a data subject on this ground, further processing is precluded.

- **Processing for scientific or historical research or statistical purposes:** Following an objection by a data subject on this ground, further processing is permitted only if the processing is necessary for the performance of a task carried out for reasons of public interest.

  The right to object must be brought to the attention of the data subject, at the time of first communication with him or her, or before. This right must be presented clearly and separately from other information. The requirement to notify data subjects of the right in this way may require revisions to privacy notices and policies.

F. Automated processing, including profiling

The GDPR provides data subjects with a right not to be subject to a decision based solely on automated processing. This is expressly stated to include profiling which is said to be a form of automated decision making. The Directive contained a similar right not to be subject to automated decision making.

The data subject's right not to be subject to a decision based solely on automated processing will not apply if the decision:

- Is necessary for entering into, or performance of, a contract between the data subject and a data controller
- Is authorised by law which lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or
- Is based on the data subject's explicit consent

Where this right applies, the data controller is required to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. The data subject must be afforded at least the right to express his or her point of view and to contest the decision.

Data subjects are entitled to be informed at the time their data is obtained by the controller of the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. Organisations will be concerned with protecting their intellectual property and know-how when making disclosures regarding the logic involved in any automated decision making and profiling.

G. Notification obligations

Following a request for rectification, restriction or erasure of personal data, the controller is required to communicate this request to all recipients to whom the personal data has been disclosed. This obligation is subject to the qualification that communication must not prove impossible or involve a disproportionate effort on the part of the controller.

The controller is also obliged to inform the data subject about those recipients if requested to do so by the data subject.

The controller must furnish information on actions taken in response to the data subject's request to exercise any of these rights without undue delay and in any event within one month of receipt of the request. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

These notification obligations are separate and additional to the requirement to make reasonable efforts to inform others who are processing data which the controller has made public and the data subject has asked to erase (described in the context of the right to erasure).

KEY TERMS AND WHERE TO FIND THEM

Data portability – Article 20
See also Recitals 68, 73, WP29 Guidance at http://bit.ly/2iAxsLI; WP29 Frequently asked questions at http://bit.ly/2kB2h3m

Erasure – Article 17 *See also* Recitals 65 - 66, 68.

Notification obligations – Articles 12(3), 17(2), 19. *See also* Recitals 59 and 62.

Objection – Article 21. *See also* Recitals 50, 59, 69 - 70, 73, 156.

Profiling – Article 4(4): Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. *See also* Recitals 71, 75.

Rectification – Article 16. *See also* Article 5 and *Recitals* 39, 59, 65, 73.

Restriction of processing – Article 18 *See also* Recital 67.

Right not to be subject to a decision based solely on automated processing – Article 22
See also Recitals 71, 75.

5.6 Privacy notices

One of the key data protection principles relates to transparency. The controller is required to take appropriate measures to provide information to a data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Typically, organisations achieve this by preparing privacy policies or notices, as well as certain 'just in time' supplemental notifications. Due to the significant new additions in the GDPR, organisations will need to update their privacy notices and policies in light of the additional information required by the GPDR.

Information obtained directly from data subject

The following information must be furnished to a data subject where the personal data is obtained directly from him or her, at the time the personal data is obtained:

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The purposes of the processing for which the personal data is intended
- The recipients or categories of recipients of the personal data
- The data retention period
- The data subject's rights to access, rectification and erasure, and
- If there will be automated decision making – together with information about the logic involved and the significance and consequences of the processing for the data subject

To these requirements the GDPR adds:

- The contact details of the data protection officer, where applicable
- The legal basis for the processing including the legitimate interests pursued by the controller or by a third party if this is the legal basis relied upon
- Information in respect of intention to transfer personal outside the EU
- The data subject's right to complain to the supervisory authority
- The data subject's rights regarding restriction of processing, objection to processing and data portability
- If processing is based on consent, the right to withdraw consent and
- Whether there is a statutory or contractual requirement to provide personal data and the consequence of failing to comply

This goes significantly beyond the Directive and will require more specific and tailored content in privacy notices than is often the case currently.

Indirectly obtained data

Where a controller obtains personal data indirectly (e.g. from a data broker or business partner), it is required to provide the data subject with the information as well as:

- The categories of information and
- The source of the information, including if it came from publicly accessible sources

In such cases, the controller is required to furnish this information:

- Within a reasonable period of having obtained the data at least within one month
- If the data is 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 is disclosed

There is no obligation to provide information to a data subject where:

- To do so would be impossible or involve a disproportionate effort
- Obtaining or disclosing the data is expressly authorised by EU or national law and which provides appropriate measures to protect the data subject's legitimate interests, or
- If the information must remain confidential, because of professional or statutory secrecy obligations, regulated by EU or national law

KEY TERMS AND WHERE TO FIND THEM

Privacy Notices (data obtained directly) – Article 13. *See also* Article 12, Recitals 58, 60 – 62.
Privacy Notices (data obtained indirectly) – Article 14. *See also* Article 12, Recitals 58, 60 – 62.

5.7 Data protection by design and default

The GDPR contains the new concepts of privacy by design and by default, intended to strengthen the protection of privacy by requiring organisations to build consideration of privacy into their product and service design processes in certain cases. The GDPR, unlike the Directive, also requires formal Data Protection Impact Assessments in relation to higher risk processing activities.

A. Privacy by design

Privacy by design requires data controllers to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to apply the data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

In ascertaining the appropriate technical and organisational measures required to be implemented the controller is required to have regard to the following:

- The state of the art
- The cost of implementation
- The nature, scope, context and purposes of processing
- The risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing

B. Privacy by default

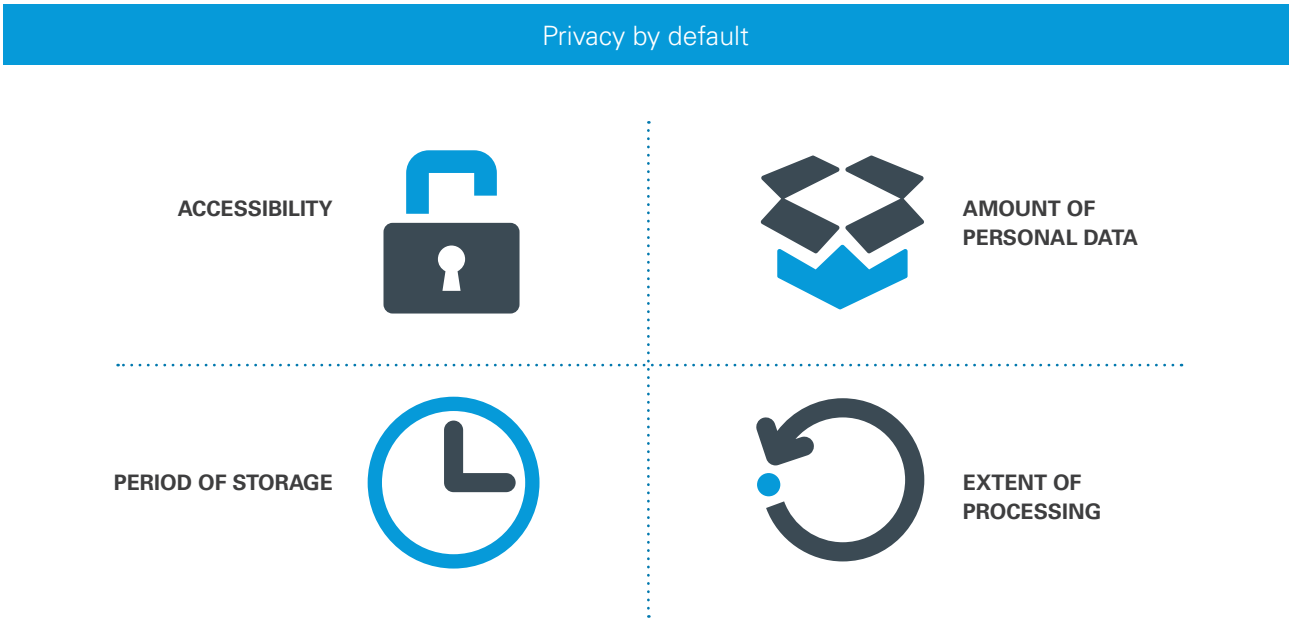
Privacy by default requires data controllers to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing are processed.

The privacy by default obligation applies to:

- The amount of personal data collected
- The extent of the processing
- The period of storage, and
- The accessibility of the data

Compliance with the requirements of privacy by default and design may be demonstrated by an approved certification mechanism.

Privacy by default and design will require organisations to review their processing activities and ensure that data protection compliance is embedded within their products and business processes.



C. Data protection impact assessments

The GDPR also makes provision for Data Protection Impact Assessments, also known as Privacy Impact Assessments ('PIAs"), which are assessments of the impact of proposed processing operations on the protection of personal data. While the Directive did not require PIAs to be carried out, the practice had emerged in a number of Member States.

The controller is required to carry out a PIA where a new processing activity is proposed, in particular, where the activity involves using new technologies and taking into account the nature, scope, context and purposes of the processing, it is likely to result in a high risk to the rights of individuals.

At a minimum a PIA must include:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller
- An assessment of whether the processing operations are necessary and proportionate in relation to the purposes
- An assessment of the risks to the rights and freedoms of data subjects, and
- The measures planned to address risks, including safeguards, security measures and mechanisms to ensure the data protection and to demonstrate compliance, considering the rights and interests of data subjects and other persons concerned.

The appropriate form of a PIA will differ to suit each organisation. However, entities which routinely process complex and large-scale personal data sets should prepare a PIA questionnaire for the use of engineers, product teams, compliance team and legal counsel.

The controller is required to consult with a supervisory authority in advance of processing where a PIA indicates that processing would result in a high risk to the rights of individuals in the absence of any measures taken by the controller to mitigate that risk

When are processing activities 'high risk'?

The GDPR does not define 'high risk', but relevant factors will be the nature, scope, context and purposes of the processing. The GDPR provides that PIAs are required in the following instances:

- Systematic and extensive evaluation of personal aspects which is based on automated processing, including profiling, and on which decisions are based that produce legal effects or similarly significantly affect the natural person
- Processing on a large scale of special categories of sensitive data or of personal data relating to criminal convictions and offences, or
- Large scale, systematic monitoring of a public area

KEY TERMS AND WHERE TO FIND THEM

Data Protection by Design and by Default – Article 25. *See also* Recital 78.
Data Protection Impact Assessment – Article 35 - 36. *See also* Recitals 84, 90 – 94.

5.8 Data protection officers

The requirement to appoint a Data Protection Officer ('DPO') will be familiar to some, but new to others, as only some national regimes require DPOs under the Directive.

Under the GDPR, it is mandatory for controllers and processors to designate a DPO in the following three instances, where:

1. The processing is carried out by a public authority or body, except for courts acting in their judicial capacity

2. The core activities of the controller or the processor consist of regular and systematic monitoring of data subjects on a large scale, or

3. The core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions

Even when the GDPR does not specifically require the appointment of a DPO, some organisations may appoint a DPO on a voluntary basis, particularly to centralise responsibility for the new compliance obligations under the GDPR.

A. Relationship between the organisation and the DPO

DPOs are not personally responsible in cases of non-compliance with the GDPR. Rather, it remains the responsibility of the controller or the processor to ensure and to demonstrate compliance with the GDPR.

The controller or the processor has a crucial role in enabling the effective performance of the DPO's tasks. DPOs must be given sufficient autonomy and resources to carry out their tasks effectively.

A group of undertakings may appoint a single DPO provided that a DPO is easily accessible from each establishment. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects, the supervisory authority but also internally within the organisation. One of the tasks of the DPO is to inform and advise the controller and the processor and the employees who carry out processing of their obligations pursuant to the GDPR.

B. Appointment and tasks of the DPO

As a first step, businesses should assess whether their organisation requires such an appointment and, if not, whether a voluntary appointment is worthwhile.

The second step is to select the right person for the role. The DPO should be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks. The DPO may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract (providing the potential to outsource the function, as company secretaries often are).

The controller or the processor must publish the contact details of the DPO and communicate them to the supervisory authority.

At a minimum a DPO is required to:

- Inform and advise the controller or the processor and the employees who carry out processing of their data protection obligations
- Monitor compliance with the GDPR and other data protection provisions
- Provide advice where requested as regards the data protection impact assessment
- Cooperate with the supervisory authority
- Act as the contact point for the supervisory authority on issues relating to processing, including prior consultation and to consult, where appropriate, with regard to any other matter

WP29 has published guidelines on DPOs, which provide further detail clarifying the circumstances in which organisations are obliged to appoint a DPO. WP29 also gives guidance on the level of expertise of the DPO. The level of expertise should be relative to the nature of data processing carried out by the organisation, and the professional qualities of a DPO are not prescriptive. WP29 also emphasises the importance of avoiding conflicts of interests and allocating sufficient resources to the DPO, among other issues.

KEY TERMS AND WHERE TO FIND THEM

Designation of DPO – Article 37. *See also* Articles 38 - 39 and Recital 97.

WP29 Guidance available at: http://bit.ly/2hNP21M

WP29 Frequently Asked Questions available at: http://bit.ly/2kaZGAt

5.9 Security

Given the potentially significant impact of security breaches on both data subjects and associated reputational damage for organisations, it is unsurprising that data security has received additional attention in the GDPR. The GDPR contains both preventative and reactive requirements in respect of personal data breaches, introducing harmonised rules around data breach notifications.

A. Reactive measures: Notification and record keeping

One of the new introductions of the GDPR is the imposition of a uniform breach notification rule. Previously, this varied in each Member State unless one operated in the telecoms sector.

In practice, the notification requirement may not amount to significant change for some data controllers. This would include Irish-established controllers. The Data Protection Commissioner's Data Security Breach Code of Practice currently mandates the reporting of such breaches and the corresponding rules under the GDPR are arguably less strict. However, the consequences for breaching the GDPR and potential heavy fines are a considerable deviation from the position under the existing Code of Practice.

Data breach notification: Supervisory authority

The GDPR adopts a risk-based approach to the requirement to notification. The controller is not required to notify the supervisory authority where the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals.

Where such risk exists, controllers are obliged to notify the competent supervisory authority of the breach. After becoming aware of the breach, the controller is required, without undue delay (within 72 hours, where feasible), to notify the personal data breach to the supervisory authority.

Where the controller fails to notify the supervisory authority within 72 hours, a reason must be furnished for this delay. Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay

Data breach notification: Processor to controller and controller to data subject

Processor to controller: Upon becoming aware of a personal data breach, processors are required to notify the controller without undue delay.

Controller to data subject: Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is required to notify the data subject of the personal data breach without undue delay.

There is no obligation to communicate a personal data breach to a data subject if any of the following conditions are met:

- The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption
- The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred is no longer likely to materialise
- It would involve disproportionate effort. In these cases, a controller should make a public communication, or similar measure, to inform data subjects in an equally effective manner

Content of notifications

At a minimum, data breach notifications to supervisory authorities and data subjects are required to:

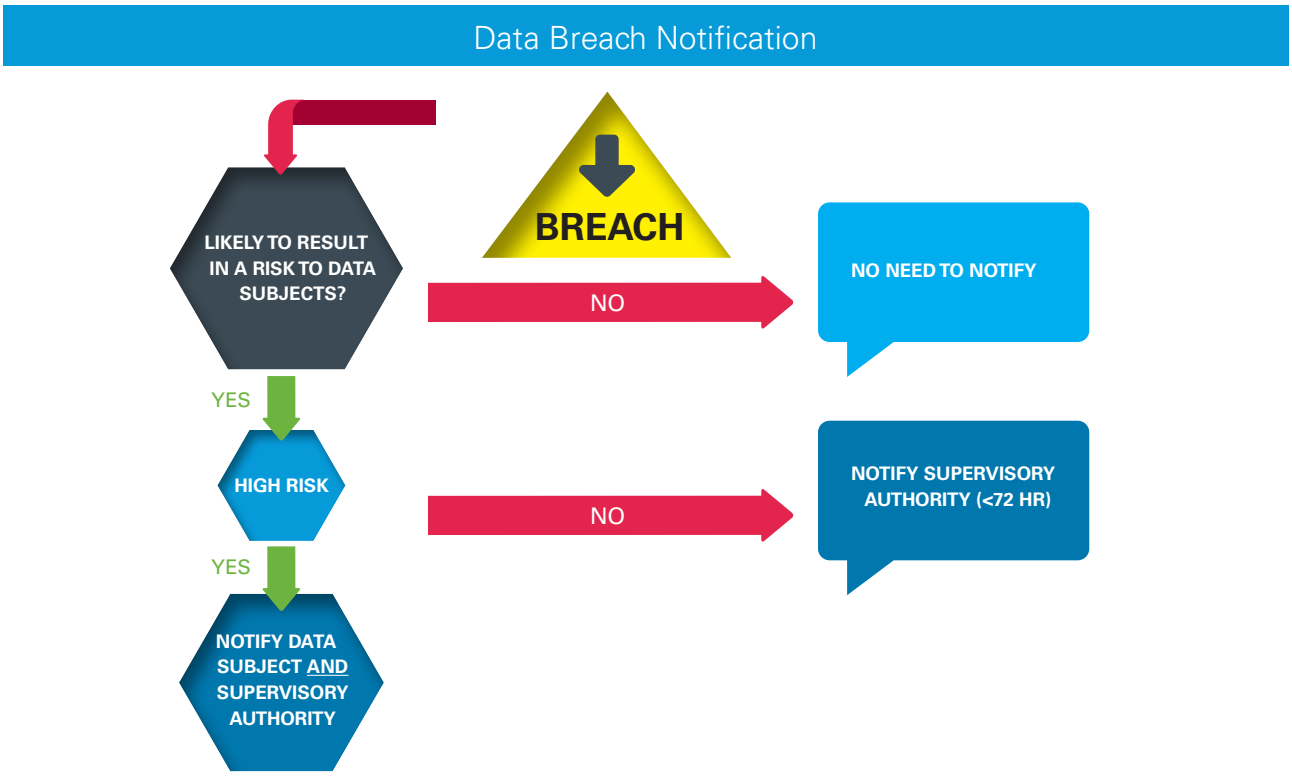
- Describe the nature of the personal data breach
- Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained
- Describe the likely consequences of the personal data breach
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach

Record keeping and policies

The GDPR also imposes record keeping obligations upon controllers, which will result in the obligation to keep a data breach register.

The controller is also required to maintain a record of any personal data breaches so as to enable the supervisory authority to verify compliance with the controller's notification obligations. Records must document the facts relating to the personal data breach, its effects and the remedial action taken.

Additionally, in order to prepare to comply with the GDPR, organisations should prepare draft template security breach notifications and security breach plans so as to be in the best position to act quickly should a breach occur.



B. Preventative measures

In addition to the requirement to report personal data breaches, the GDPR also requires preventative measures. As is required under the Directive, controllers and processors must implement 'appropriate technical and organisational measures' to ensure a level of security appropriate to the risk presented by the processing.

Technical and organisational measures, which should be implemented as appropriate, include:

- The pseudonymisation and encryption of personal data
- The ability to ensure the on-going confidentiality integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Conforming to an approved code of conduct or an approved certification mechanism may be used to demonstrate compliance with these security requirements. Controllers and processors are also required to take steps to ensure that any individual acting under its authority who has access to personal data does not process that data other than in accordance with instructions from the controller, unless he or she is required to do so by law.

While the rules with regard to preventative security measures are largely unchanged, due to the increased potential for fines, and the ability for individuals to recover compensation for non-material loss, the potential risks of ignoring security have become much greater.

KEY TERMS AND WHERE TO FIND THEM

Personal Data Breach - Article 4(12) – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. *See also* Recitals 73, 75, 85 – 88.

5.10 Enforcement, remedies and liability

Some of the most significant changes seen under the GDPR relate to enforcement, remedies and liability. National supervisory authorities are granted significant powers. Plaintiffs will be able to sue in their national courts and recover compensation without the need to demonstrate material damage. As a result, the potential negative consequences of non-compliance with data protection law are much higher under the GDPR than previously seen.

A. Role of supervisory authorities

Similar to the Directive, the enforcement of the GDPR is the responsibility of the supervisory authority (also commonly known as 'data protection authorities'). Each Member State is required to appoint at least one supervisory authority for the purposes of monitoring the application of the GDPR.

The GDPR contains an extensive list of tasks for each supervisory authority. Supervisory authorities also have a broad mandate to fulfil any other tasks related to the protection of personal data. The powers of supervisory authorities are correspondingly broad.

Each Member State is required to provide, by law, that its supervisory authority shall have the power to bring infringements of GDPR to the attention of the judicial authorities and where appropriate, to bring legal proceedings in order to enforce the provisions of the Regulation. Member States can also give additional powers to supervisory authorities.

The GDPR obliges controllers and processors to maintain records of both compliance with and breaches of the GDPR and to furnish these to the supervisory authority on request.

B. 'One-stop-shop'

One of the central pillars of the GDPR is the 'one-stop shop'. The concept aims to facilitate multinational companies by allowing them to deal with a single supervisory authority, even where they have a number of establishments across the EU. The original European Commission proposal was that the supervisory authority for the country where the controller had their 'main establishment' would be the sole authority for monitoring and ensuring compliance by that controller throughout the EU. However, the GDPR as adopted contains a diluted version of that original one-stop shop concept.

The GDPR provides that controllers and processors engaged in cross-border processing are to be regulated by the supervisory authority in the Member State where they have their 'main establishment'. Generally, the main establishment is the place of central administration of the controller in the EU. However, if data protection decision-making occurs elsewhere in the Union, the establishment where such decision-making takes place is the main establishment.

The authority in the Member State of the main establishment will be the 'lead supervisory authority'. This lead supervisory authority has the power to regulate that controller or processor across all Member States, to the extent that its data processing activities involve cross-border data processing.

Individuals are entitled to lodge a complaint with any supervisory authority. That authority must inform the lead supervisory authority, which will in turn determine whether it will handle the complaint. If the lead supervisory authority decides not to handle the complaint itself, the supervisory authority to whom the complaint was made will handle it.

The European Data Protection Board ('EDPB') is a body established under the GDPR, replacing the WP29. Similar to the WP29, it comprises the head or representative of one supervisory authority from each Member State and of the European Data Protection Supervisor ('EDPS'). The European Commission also has a non-voting right to participate on the Board. The EDPB has a lengthy list of tasks. Unlike the WP29, which was an advisory committee, the EDPB will have a more formal and robust set of tasks relating to the enforcement of data protection law. The primary obligation of the EDPB is to ensure the consistent application of the GDPR throughout the EU.

The consistency mechanism

In order to deal with scenarios where more than one supervisory authority may be concerned with a complaint/investigation, the GDPR provides for mandatory co-operation by supervisory authorities under the consistency mechanism. The aim of this mechanism is to ensure the uniform application of the GDPR across the EU. There are exceptions from this mechanism in cases of urgency.

This co-operation takes the form of the sharing of information by the lead supervisory authority and the attempt to come to a decision by consensus, in a process whereby the lead supervisory authority issues a draft decision to the other concerned authority. In cases where the lead supervisory authority disagrees with the views of the other concerned authorities, the investigation must be referred to the EDPB.

C. Remedies

The GDPR affords data subjects with the following remedies:

Right to lodge a complaint with a supervisory authority

- The data subject may lodge a complaint with a supervisory authority, if he or she considers that his or her data has been processed unlawfully.
- The supervisory authority is obliged to inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy.

Right to an effective judicial remedy against a supervisory authority

- Individuals have the right to an effective judicial remedy in respect of legally binding decisions of supervisory authorities concerning him or her (e.g. appeal to a national court).
- Data subjects have the right to an effective judicial remedy for a failure by a supervisory authority to handle a complaint or a failure to inform the data subject within three months on the progress or outcome of his or her complaint.

Right to an effective judicial remedy against a controller or processor

- Data subjects have the right to an effective judicial remedy against a responsible controller or processor where the data subject considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR.

Right to compensation and liability

- Any person who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor for the damage suffered. The extension of the right to compensation to cover non-material damage is significant, and a departure from some national regimes.

- Both controllers and processors may be liable for compensation under the GDPR. Controllers are liable for the damage caused by processing which infringes the GDPR. Processors are liable for the damage caused by processing in breach of their GDPR obligations or where processing is carried out outside or contrary to the lawful instructions of the controller.

- In order to ensure effective compensation of the data subject where more than one data controller or processor is responsible for the damages, each controller or processor may be held liable for the entirety of the damages. However, where a controller or processor has paid full compensation for the damage suffered, it may subsequently bring proceedings against the other parties to recover their portions of the damages.

- The GDPR also regulates joint data control. Where two or more controllers jointly determine the purpose and means of processing they are regarded as joint controllers and data subjects may enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages.

- A controller or processor is exempt from liability under the GDPR if it can prove that it is not in any way responsible for the event giving rise to the damage. This exemption is somewhat narrower than the wording of the Directive, which exempts a controller from liability upon proof that it is 'not responsible for the event giving rise to the damage'. Under the GDPR, to ensure effective compensation, each controller or processor that is involved in unlawful processing and responsible for harm caused to a data subject will be held liable for the entirety of the harm caused as a result. In other words, the GDPR provides for joint and several liability against all potentially responsible parties if they are in any way liable for the breach, so a processor which is responsible for 1% of the liability could be required to pay 100% of the damages.

- Organisations engaged in joint data control should contractually determine the apportionment of liability so as to limit the scope for dispute at a later stage.

D. Administrative fines

Currently, the power to impose fines for breaches of data protection law varies across the EU. For example, under the Data Protection Acts 1998 and 2003 only the Courts, and not the Data Protection Commissioner, can levy fines.

The GDPR envisages the imposition of fines by a supervisory authority in addition to or instead of other corrective measures. Supervisory authorities are required to ensure that administrative fines imposed are 'effective, proportionate and dissuasive'.

The GDPR contains two thresholds for administrative fines, which depend on the specific data protection obligation which has been breached. The lesser threshold sees fines of up to €10 million or 2% of the undertaking's total worldwide annual turnover of the preceding financial year, whichever is greater, being imposed. The higher level of fine is up to €20 million or 4% of the undertaking's total worldwide annual turnover of the preceding financial year, whichever is greater. An 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which govern EU competition law. These Articles construe the term broadly and as such it appears that group revenues may be used by supervisory authorities when calculating administrative fines.

Administrative Fines

€10 million or **2%**	€20 million or **4%**
Conditions for obtaining a child's consent	The core data protection principles
Processing which does not require identification	The lawful processing conditions
Data protection by design and default obligations	The conditions for consent
Designating a representative in the State where the controller is not established in the EU	The sensitive personal data processing conditions
Obligations of processors	Data subjects' rights (including information, access, rectification, erasure, restriction of processing, data portability, objection, profiling)
Instructions of a controller or processor	Transfers of data to third countries
Records of processing	Failure to provide access to premises of a controller or processor
Cooperation with the supervisory authority	Compliance with a specific order or limitation on processing by the supervisory authority or the suspension of data flows
Security measures	Obligations adopted under Member State law in regard to specific processing situation
Notification of a personal data breach to the supervisory authority	
Communication of a personal data breach to the data subject	
Conducting PIAs and prior consultation	
Designation, position and tasks of the DPO	
Monitoring of approved codes of conduct	
Certification mechanisms	

In ascertaining the level of fine to impose in a given case the supervisory authority is obliged to have regard to the following factors:

- The nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them
- The intentional or negligent character of the infringement
- Any action 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 by the controller or processor
- The degree of cooperation with the supervisory authority
- The categories of personal data affected
- The manner in which the infringement became known to the supervisory authority
- Where measures have previously been ordered against the controller or processor concerned with regard to the same subject matter, compliance with those measures
- Adherence to approved codes of conduct or approved certification mechanisms, and
- Any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions, the total amount of the administrative fine may not exceed the amount specified for the most serious infringement. In other words, if a single wrongful act amounts to non-compliance with more than one provision of the GDPR, the maximum fine is still €20 million or 4%.

KEY TERMS AND WHERE TO FIND THEM

One-stop-shop – Recitals 124-138 and Chapter VII, Section 182.

5.11 Codes of conduct and certification

A. Codes of conduct

The GDPR, in similar language to the Directive, requires Member States, supervisory authorities, the EDPB and the Commission to encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR.

Such codes of conduct could address the exercise of the rights of data subjects, general data protection obligations and notification of data breaches.

Adherence to an approved code of conduct can be evidence of compliance with a controller or processor's GDPR obligations or provide the basis for cross-border data transfers.

B. Certification

Similarly, the GDPR requires Member States, supervisory authorities, the EDPB and the Commission to encourage the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with the GDPR.

Certification processes must be voluntary and available through a transparent process. Certification will be issued by certification bodies or by supervisory authorities on the basis of criteria approved by that supervisory authority. Where the criteria are approved by the EDPB, this may result in a common certification, the European Data Protection Seal.

KEY TERMS AND WHERE TO FIND THEM

Administrative fines – Article 83. *See also* Recitals 150, 152.

Cross-border processing – Article 4(23) - Either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

European data protection board – Articles 64, 68. *See also* Articles 94, 132 – 134.

Exemption from liability – Article 82(3). *See also* Recital 146.

Joint controllers – Article 26(3) . *See also* Recitals 82(3) – (5), Recitals 49, 146.

Main establishment (controller) – Recital 36 - The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements.

Main establishment (processor) – Recital 36 - The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union.

Right to lodge a complaint with a supervisory authority – Article 77. *See also* Recital 141.

Right to an effective judicial remedy against a supervisory authority – Article 78. *See also* Recital 143.

Right to an effective judicial remedy against a controller or processor – Article 79. *See also* Recital 143.

Right to compensation and liability – Articles 77 – 82. *See also* Recitals 146 – 147.

Supervisory authority - Article 4(21) - An independent public authority which is established by a Member State pursuant to Article 51.

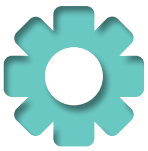
Supervisory authority concerned – A supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority.

Codes of conduct – Articles 40, 41.

See also Articles 24, 28, 35, 46, 57, 58, 64, 83 and Recitals 77, 81, 98 – 99.

Certification – Articles 42, 43. *See also* Recitals 77, 81,100.

6. What does the GDPR mean for ... ?



6.1 Contracting

Data protection clauses and addendums have been included in commercial contracts for some time, but the GDPR will significantly increase the importance of incorporating appropriate data protection language into contracts.

The three aspects of the GDPR of particular importance for consideration in drafting contracts are:

- The transfer of data to a third country
- The engagement of processors and sub-processors
- The rules in respect of liability

A. Data exports

Data transfers have caused increasing difficulties for organisations since the invalidation of Safe Harbor in Schrems v Data Protection Commissioner (C-362/14), and the uncertainty this has created. The GDPR does not represent any great salvation from this uncertainty, as it largely follows the same template as the regime under the Directive. Contractual solutions are likely to continue to play a significant role in solving export issues.

With regard to the transfer of personal data outside the European Economic Area, the GDPR, like the Directive, prohibits such transfers unless, one of three types of measure is in place:

- That the third country (or a certification mechanism in that country) has been deemed adequate by the European Commission
- The controller ensures appropriate safeguards are in place, or
- A specific derogation is in place

Adequacy

- Commission designated or 'white-listed' countries (e.g. Canada, New Zealand)
- Commission designated self-certification schemes (EU-US Privacy Shield)

Appropriate Safeguards

- Binding, enforceable instrument between public authorities
- Binding corporate rules
- Standard data protection clauses (know today as Standard Contractual Clauses and also referred to as Model Clauses)
- Approved code of conduct and enforceable commitments
- Approved certification mechanism and enforceable commitments

Derogation

- Explicit consent to the transfer
- Necessity for the performance of a contract
- Necessity for reasons of public interest
- To establish, exercise or defend legal claims
- To protect vital interests, if the data subject is incapable of consenting
- Transfer from certain public registers
- Compelling legitimate interests

Notably, in relation to the consent derogation, the GDPR replaces the requirement of unambiguous consent, which prevailed under the Directive, with a requirement for explicit consent. Binding corporate rules are put on express legislative footing, after having developed under the Directive in accordance with a national supervisory authority's ability to authorise transfers. The ability to transfer data on the basis of an organisation's legitimate interests is also a significant addition but instances when this derogation can be used are quite curtailed.

The GDPR further provides that any judgment of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised and enforceable if based on an international agreement, such as a mutual legal assistance treaty. This would seem to be targeting the Microsoft v USA warrant case scenario, where a national court in the US ordered the disclosure of personal data held in an Irish data centre.

B. Engagement of processors and sub-processors

Organisations who engage service providers to process personal data on their behalf (e.g. outsourcing payroll processing or engaging with a third party for data storage) may be familiar with the requirement to enter into processing agreements under the Directive. The scope of obligations to be included in such data processing agreements has been significantly expanded under the GDPR.

Where processing is carried out on behalf of a controller, the controller may only engage processors who provide sufficient guarantees to implement appropriate technical and organisational measures to comply with the GDPR and ensure the protection of the rights of the data subject. The GDPR expressly requires that a large number of clauses be included in a processing contract between the controller and the processor, including obligations relating to confidentiality, security, sub-processing, security breach notification and deletion.

When it comes to sub-processing, these obligations must be flowed down to that contractor in a sub-processing agreement. The appointment of sub-processors, a topic which was not expressly addressed by the Directive, is also specifically regulated by the GDPR. The GDPR provides that a processor may not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor is required to inform the controller of any intended changes concerning the addition or replacement of other processors, giving the controller the opportunity to object to such changes. Sub-processors are subject to the same requirements that the GDPR imposes on the original processor and they are bound by any contracts with the controller.

In a digital world, where certain functions are commonly outsourced to third party providers, involving many sub-processors, contracting has just become more challenging. Many existing agreements may need to be renegotiated, in order to accommodate the GDPR's requirements.

C. Joint controllership contracts

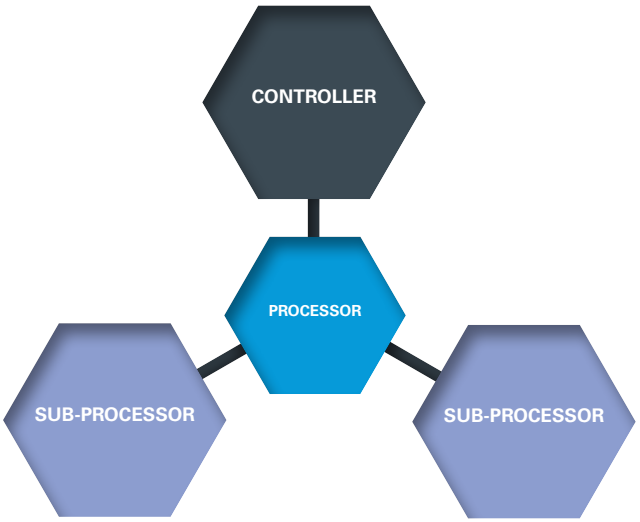
A new requirement introduced by the GDPR, not previously seen under the Directive, is the requirement to put contracts in place between joint controllers. The arrangement between the controllers should reflect the respective roles and relationships of the joint controllers, in particular relating to the allocation of responsibility for compliance obligations under the GDPR (including providing notice to data subjects and ensuring data subjects' rights are met).

D. Liability

The GDPR departs from the Directive in providing for joint and several liability between controllers and processors, and between joint controllers. As a consequence, it is important that contracts contain an appropriate apportionment clause and indemnities to protect a party from being left out of pocket in relation to damage caused by a contracting party, and to provide for dispute resolution mechanisms.

Where a sub-processor fails to fulfil its data protection obligations, the initial processor will remain fully liable to the controller. Therefore processors who sub-contract their obligations must be similarly cautious and include appropriate contractual provisions to safeguard their position.

Sub-Processing Structure



KEY TERMS AND WHERE TO FIND THEM

General principle for transfer – Article 44. *See also* Recital 101 – 116

Adequacy decisions – Article 45. *See also* Recital 103 – 107

Appropriate safeguards – Article 46

Derogations – Article 49. *See also* Recitals 111 – 112

Joint controllers – Article 26

Processor – Article 28

Transfers and disclosures not authorised by EU law – Article 48. *See also* Recital 115

CASE STUDY

Green White & Orange is an accountancy firm established in Ireland. It engages a Canadian company, Maple Inc., to deliver cloud-based storage services. Green White & Orange is the controller in this instance as it controls what data is sent to the cloud and for what purpose, and Maple Inc. is a processor.

As Maple Inc. is located outside the European Economic Area, the transfer of data to them will be a data export. Consequently, the transfer can only take place where appropriate safeguards are in place, where the transfer is permitted owing to an adequacy decision of the Commission or a derogation (such as consent) is available.

Should the current Commission adequacy decision for Canada be renewed under the GDPR, Green White & Orange may be able to avail of that basis for the transfer. Alternatively, it could choose to put in place standard contractual clauses to provide appropriate safeguards.

At the same time as relying on the Commission's Canadian adequacy decision, a processing contract must be put in place between both parties, setting out the obligations to which Maple Inc. will be subject as a processor.The parties should also assess an appropriate division of liability between the parties and reflect this position in a liability clause.

6.2 Compliance & risk management

One of the biggest changes for organisations under the GDPR is the compliance burden it imposes with the introduction of the 'accountability' principle. Controllers and processors are now required to be able to demonstrate their own compliance. Organisations need to implement accountability processes, appropriate record keeping and may need to appoint a DPO.

Evolution of data protection compliance

The GDPR demonstrates that data protection legislation is evolving in the same way that financial services regulation has over the recent years. 'Conduct risk' is a newer category of risk for financial services firms and a focus of both Irish and UK regulators. In essence, regulators expect to see evidence of firms embedding a consumer-centred culture from the top of the organisation right through to the staff delivering products and services, going beyond 'tick-box' compliance.

The GDPR is similar in this regard. The concepts of data protection by design and default, along with the requirement to conduct a PIA in certain cases, suggest that data protection should be central to all change management projects in an organisation. Data protection risk and compliance must become part of business-as-usual, in much the same way as general risk and compliance has become. In particular, for both new and existing products or services which involve the processing of personal data, organisations must ensure that the relevant product or service is designed with data protection compliance in mind.

The Role of the DPO

The DPO must be able to act in an independent manner. The GDPR has introduced safeguard provisions for the role of the DPO (where one is required), similar in nature to provisions protecting the independence and autonomy of the role of the Chief Risk Officer or Chief Compliance Officer. In particular, DPOs cannot be directed by organisations on how to perform their duties or what the outcome of their decisions may be, nor can they be penalised for such performance. While DPOs can also be responsible for other functions in an organisation, a DPO may not be assigned tasks or duties which would result in a conflict of interest. DPOs should be actively supported by senior management, and should report to the highest level of management within the organisation, to ensure that the rights of data subjects are part of all strategic risk conversations in the boardroom.

Record Keeping

The GDPR requires controllers and processors to maintain a record of processing activities. The records maintained must be in writing (electronic is sufficient). Such records must be made available to the supervisory authority upon request. Records maintained by the controller must contain the following information:

- The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer
- The purposes of the processing
- A description of the categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data has been or will be disclosed including recipients in third countries or international organisations
- Details of transfers of personal data to a third country and the appropriate safeguards
- The envisaged time limits for erasure of the different categories of data
- A general description of the technical and organisational security measures in place

SME exemption

- *Controllers and processors employing less than 250 employees are not required to maintain such records, unless the processing is likely to result in a risk to rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive data or personal data relating to criminal convictions and offences.*

The records maintained by the processor must contain the following information:

- The name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer
- The categories of processing carried out on behalf of each controller
- The details of transfers of personal data to a third country and the appropriate safeguards
- A general description of the technical and organisational security measures in place.

With regard to security, the GDPR imposes additional record-keeping obligations on the controller. Controllers are required to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

An integrated approach to compliance

As most of the requirements of the GDPR are interlinked and interdependent, the changes they bring cannot and should not be effected in a piecemeal fashion. Organisations will have to undertake a gap analysis of their existing data protection control environment against the new requirements. This document should, in detail, understand what personal data they have, why they have it, and who and where they transfer it to, particularly given the extraterritorial scope of the GDPR. Most organisations will likely, at a minimum, have to refresh their fair processing notices and rethink consent capture mechanisms. For many organisations, this will mean revising data protection wording on websites, online application forms, interactive voice recordings, call centre scripts, proposal and application forms, renewal notices and annual account statements.

Where changes are required, organisations will have to ring-fence old data (data obtained pre-GDPR) and new data (GDPR-compliant data), in order to determine the extent of permissible processing activities for data sets.

KEY TERMS AND WHERE TO FIND THEM

Records of processing activities – Article 30. *See also* Recital 82.

6.3 Human resource managers

From the perspective of Human Resource Managers, the ability of Member States to legislate more specifically than the GDPR does, in respect of the processing of personal data, as well as the changes implemented in respect of data subject requests, will be of particular note.

National variations

Unlike the harmonisation seen in many other areas of the GDPR, in the employment sphere we may continue to see considerable differences. This is because the GDPR allows Member States to, by law or by collective agreements, provide for more specific rules in respect of the processing of employees' personal data in the employment context.

This is particularly the case for the purposes of the recruitment and the performance of the contract of employment, including:

- Discharge of obligations laid down by law or by collective agreements
- Management, planning and organisation of work
- Equality and diversity in the workplace
- Health and safety at work
- Protection of employer's or customer's property
- For the purposes of the exercise and enjoyment of rights and benefits related to employment
- For the purpose of the termination of the employment relationship

As a result, national variations in practices are going to continue, and organisations are likely to face varying requirements with respect to the processing of personal data of employees between one Member State and another, rather than being able to adopt one uniform approach.

Obtaining employee consents and updating policies

Obtaining valid consents from employees has always been challenging due to the imbalance of power between the parties, leading to a suspicion by some national supervisory authorities that such consents are not freely given. The conditions for obtaining consent have now become stricter, as has been described elsewhere in this guide. Consequently, employee consent forms and processes will need to be updated.

In light of new transparency obligations, employee data protection notices will also need to be updated, and IT / Acceptable Use Policies may also need revisiting.

Subject access requests

The changes in the law in respect of subject access requests will also be of note to HR Managers as subject access requests are frequently used as a pre-litigation tool in employment disputes. Changes are made in respect of the content of the information required to be furnished, the response time and the ability to charge a fee.

CASE STUDY

Organisation Yellow is a professional services firm. An employee, John Doe, is involved in a grievance procedure and requests all data that that Organisation Yellow holds in respect of him. Organisation Yellow has employed John Doe for over ten years, and holds a large volume of personal data about him. Organisation Yellow, owing to this large volume, is entitled to respond to this request requiring him to specify the information to which the request relates.

Organisation Yellow is also permitted, owing to the large volume of personal data retained, to extend the one month time period in respect of which it is required to reply, provided this is communicated to John Doe within one month of Organisation Yellow having received the request. When furnishing the data subject with the information sought, Organisation Yellow is required to provide this information in a written format. Upon receipt of this information, John Doe requests a further copy. Organisation Yellow is entitled to charge a reasonable fee only in respect of the further copy sought him.

Limitations

As under the Directive, the GDPR provides that the right of access should not adversely affect the rights of others. Limitations to the rights to access are therefore still envisaged under the GDPR, which expressly provides that this could extend to protection of trade secrets or intellectual property and in particular the copyright protecting the software. Nonetheless, the result of those considerations should not be a refusal to provide all information to the data subject.

In addition, the rights of data subjects, including the right of access, may be restricted, by legislative measures where such restriction respects fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- National security
- Defence
- Public security
- The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties
- Other important objectives of general public interest
- The protection of judicial independence and judicial proceedings
- The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions
- A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority
- The protection of the data subject or the rights and freedoms of others
- The enforcement of civil law claims

However, until we see the exemptions which each Member State chooses to implement, there will be continued uncertainty as to the scope of these exemptions.

How will subject access requests change under the GDPR?

Change	*Directive*	*GDPR*
Content	• The purposes of the processing • The categories of personal data concerned • The recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organisations • Where the personal data is not collected from the data subject, any available information as to their source • The existence of automated decision-making, including profiling, and the logic involved	In addition to the information required by the Directive: • The data retention period • The data subject's right to rectification, erasure, restriction or objection to processing • The right to lodge a complaint with a supervisory authority • The significance and the envisaged consequences of automated decision-making for the data subject • Where personal data is transferred to a third country or to an international organisation, the appropriate safeguards
Response Time	*40 Days*	*One Month (may be extended by two months where necessary)*
Fees	• Permissible to charge a fee of €6.35	• Generally no fee may be charged • A reasonable fee may be charged for further copies • A reasonable fee may be charged where a request is manifestly unfounded or excessive

KEY TERMS AND WHERE TO FIND THEM

Processing in the context of employment – Article 88. *See also* Recital 155.
Subject access requests – Articles 12(5), 15. *See also* Article 23, Recitals 59, 63.

6.4 Technology-driven businesses

Technology-driven businesses, particularly those which routinely process large personal data sets, should be aware of a number of changes to data protection law in light of the GDPR. Two points of particular relevance are the challenges faced by businesses in obtaining consent and the extension in the rights afforded to data subjects under the GDPR.

A. Consent

Processing is lawful only where there one of the legal bases for processing is present, including on the basis of consent.

For some technology businesses, the increased standards applicable to consent will make obtaining consent more challenging.

For example, providers of internet of things or smart devices may not always have an online sign-up process with all data subjects whose data they process. The lack of a direct relationship can make capturing and demonstrating an adequate consent challenging.

In order to comply with the GDPR, it will be necessary to demonstrate that consent is specific, freely given, informed and an unambiguous indication of the data subject's wishes by a statement or clear affirmative action. Compliance with this requirement will be fact-specific.

Difficulties may be encountered where processing has multiple purposes. For software app providers, for example, personal data may be processed for multiple purposes such as advertising, provision of the service, and research and development purposes. The GDPR requires that consent should be obtained for each of these individual purposes and a single combined consent will present challenges.

Providers of information society services routinely used by children between 13-18 years of age may need to develop special 'child-friendly' privacy policies, and due to the potential for variation across Member States in relation to the age of consent, different terms of use (or at least variations to terms of use) may be needed in different Member States.

Together with the need to amend standard terms of service and privacy policies, technology driven businesses may also need to consider develop innovative means of capturing consent on a per-purpose basis.

B. Rights of data subjects

For technology-driven businesses, a data subject's right to data portability and erasure are of particular importance.

Data portability

Data subjects have a right to receive a copy of the personal data they provided to a controller in a commonly used, machine-readable format and a right to transfer their personal data from one controller to another or have the data transmitted directly between controllers.

In order to facilitate data subjects in the exercise of this right, controllers and processors will be required to develop procedures and tools so as to comply with the requests of data subjects. Given the expansive interpretation the WP29 has of the data in scope (extending to both data directly provided, and data generated in relation to the data subject's activity), controllers will have to think about developing special tools. The WP29 has suggested that APIs should be developed to facilitate the transmission of relevant data to another data controller. This will be challenging due to lack of inter-operability of competing services, however, the WP29 recommends co-operation on a common set of interoperable standards.

Importantly, businesses are not obliged to respond to data portability requests where to do so would compromise their own trade secrets or intellectual property.

Erasure

It is important for technology driven businesses to ensure that their database architecture facilitates deletion. As data controllers are also required to make reasonable efforts that information relating to a data subject is erased not only on their systems, but also that of third-party systems, that have copied, replicated or linked to the original information. Building in processes for notifying third parties should also be considered.

6.5 Disputes/Litigation

A number of provisions of the GDPR will be of note from a litigation perspective. The in-house lawyer, in particular, will be required to understand the procedural rules introduced by the GDPR in respect of jurisdiction and parallel proceedings as well as the role of the competent supervisory authority.

Engaging with the Supervisory authority

Supervisory authorities are responsible for the enforcement of the GDPR.

In respect of processing which does not have a cross-border element, the roles and responsibilities of supervisory authorities remain largely the same as under the Directive. Consequently, controllers and processors may continue to rely upon their existing experience of interactions with supervisory authorities. Where there is a **cross-border element** to an organisation's processing activities, the controller or processor will be subject to regulation by the supervisory authority in the Member State in which the controller or processor has its main establishment. Relationship building efforts should therefore be focused on the jurisdiction in which a controller or processor's lead supervisory authority is based. Nonetheless, engagement with local supervisory authorities will remain important owing to the co-operative relationship between lead and concerned supervisory authorities.

Jurisdiction issues in civil litigation

The GDPR affords a data subject the following remedies:

- Right to lodge a complaint with a supervisory authority
- Right to an effective judicial remedy against a supervisory authority
- Right to an effective judicial remedy against a controller or processor
- Right to compensation

Each right is exercisable subject to specific rules that determine which Member State's courts have jurisdiction over a given dispute. Of particular note from a civil litigation perspective are the rights to an effective judicial remedy against a controller or processor and the right to compensation. These rights entitle a data subject to initiate proceedings against a controller or processor, in cases where non-compliant processing of personal data has led to an infringement of his or her rights, and to potentially recover compensation for material or non-material damage due to the breach.

In terms of the forum, proceedings against a controller or a processor can be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Consequently, controllers and processors may be required to attend court in the country where a data subject has his or her habitual residence, as opposed to the country where the controller or processor has its establishment. Organisations which provide services to data subjects across the EU could expect to potentially be sued in any of the Member States. These rules are similar to the EU rules in relation to consumer law claims.

Set out below is a summary of the main rules in respect of forum:

RIGHT	FORUM
Lodge a complaint with a supervisory authority	Member State of the data subject's habitual residence, place of work or place of the alleged infringement
An effective judicial remedy against a supervisory authority	Courts of the Member State where the supervisory authority is established
An effective judicial remedy against a controller or processor (including compensation)	Courts of the Member State where the controller or processor has an establishment or courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers

6.6 Public sector bodies

The GDPR will affect how public bodies use personal data in a number of key ways. Four points of particular relevance are:

- the grounds on which public bodies may process personal data
- the requirement to appoint a DPO
- the introduction of PIAs, and
- the applicability of the rules regarding the lead supervisory authority

A. Grounds for processing personal data

Currently, public bodies can process personal data where the processing is necessary for the purposes of the data controller's legitimate interests, as well as other lawful grounds. Under the GDPR, the 'legitimate interests' ground will no longer be available to public authorities to justify the processing of personal data. Instead, public authorities will have to establish an alternative legal ground for processing personal data.

As was the case under the Directive, public authorities continue to be allowed to process personal data where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

It will also be more difficult for public bodies to rely on consent as a legal basis for data processing under the GDPR. The GDPR is clear that consent does not provide a valid legal ground for the processing of personal data in cases where there is a clear imbalance between the data subject and the data controller, in particular where the data controller is a public authority.

There is also an express basis allowing the disclosure of data contained in official documents, held by a public body for the performance of a task carried out in the public interest. Such personal data may be disclosed by the body in accordance with Irish or EU law to which the body is subject. This is in order to reconcile public access to official documents with data protection rights.

B. Data protection officers

Under the GDPR, public sector bodies, other than courts acting in their judicial capacities, are obliged to appoint a DPO. Public sector bodies are permitted to share DPOs, taking account of their size and organisational structure.

C. Data protection impact assessments

Data controllers are required to carry out PIAs where data processing activities are likely to result in a 'high risk' to the rights and freedoms of natural persons. Such risks may arise for public bodies, due to their processing of large amounts of personal data that is often sensitive in nature. PIAs will assist public bodies in identifying and understand current and new risks in their processing of personal data.

PIAs are obligatory in the following circumstances, which are particularly relevant to public authorities:

- Where a systematic and extensive evaluation of personal aspects relating to data subjects which is based on automated processing, including profiling, and on which decisions are made about data subjects that legally affect them or significantly affect them
- Processing on a large scale of sensitive personal data or data on criminal convictions and offences, and
- Systematic monitoring of publicly accessible areas 'on a large scale'

The GDPR recognises that there are circumstances in which it may be reasonable and economical for the subject of a PIA to be broader than a single project, for example where public bodies intend to establish a common application or processing platform.

D. Lead supervisory authority

The rules on the lead supervisory authority and the one-stop-shop mechanism, do not apply where the processing is carried out by Irish public bodies in the public interest. In such cases, the only supervisory authority competent to exercise the powers conferred to it in accordance with the GDPR is the supervisory authority of the same Member State. For example, only the Irish Data Protection Commissioner would be competent to supervise an Irish public body's data processing activities in cases of public interest.

KEY TERMS AND WHERE TO FIND THEM

Consent – Recital 43.

Data protection impact assessment – Article 35(3). *See also* Recital 92.

Data protection officer – Article 37(1)(a), 37(3). *See also* Recital 97.

Lead supervisory authority – Article 41. *See also* Recital 128.

Grounds for processing personal data – Article 6 (1) para. 2, (6)(1)(e), 86. *See also* Recitals 10, 45, 69, 154.

7. Our experts

Privacy & Data Security

Philip Nolan
Partner
pnolan@mhc.ie
+353 1 614 5078

Mark Adair
Partner
madair@mhc.ie
+353 1 614 2345

Wendy Hederman
Partner
whederman@mhc.ie
+353 1 614 5857

Robert McDonagh
Partner
rmcdonagh@mhc.ie
+353 1 614 5077

Oisín Tobin
Partner
otobin@mhc.ie
+1 415 655 6841

Jevan Neilan
Senior Associate
jneilan@mhc.ie
+353 1 614 5875

Áine Cadogan
Associate
acadogan@mhc.ie
+353 1 614 7728

Ailbhe Durkin
Associate
adurkin@mhc.ie
+353 1 614 2312

Meabh Earlie
Associate
mearlie@mhc.ie
+353 1 614 7731

Emily Mahoney
Associate
emahoney@mhc.ie
+353 1 614 2396

Richard McNally
Associate
rmcnally@mhc.ie
+353 1 614 2386

Áine Quirke
Associate
aquirke@mhc.ie
+353 1 614 2495

Emmie Tran
Consultant
etran@mhc.ie
+1 415 655 6841

Liam Walsh
Associate
lwalsh@mhc.ie
+353 1 614 5086

Privacy Litigation

Richard Woulfe
Partner
rwoulfe@mhc.ie
+353 1 614 5070

Lucy Craze
Senior Associate
lcraze@mhc.ie
+353 1 614 2316

Eimear O'Brien
Associate
eobrien@mhc.ie
+353 1 614 5052

Ciaran O'Neill
Associate
ciaranoneill@mhc.ie
+353 1 614 2456

Public Sector Privacy

Catherine Allen
Partner
callen@mhc.ie
+353 1 614 5254

Niall Michel
Partner
nmichel@mhc.ie
+353 1 614 5014

Lisa Joyce
Senior Associate
ljoyce@mhc.ie
+353 1 614 5228