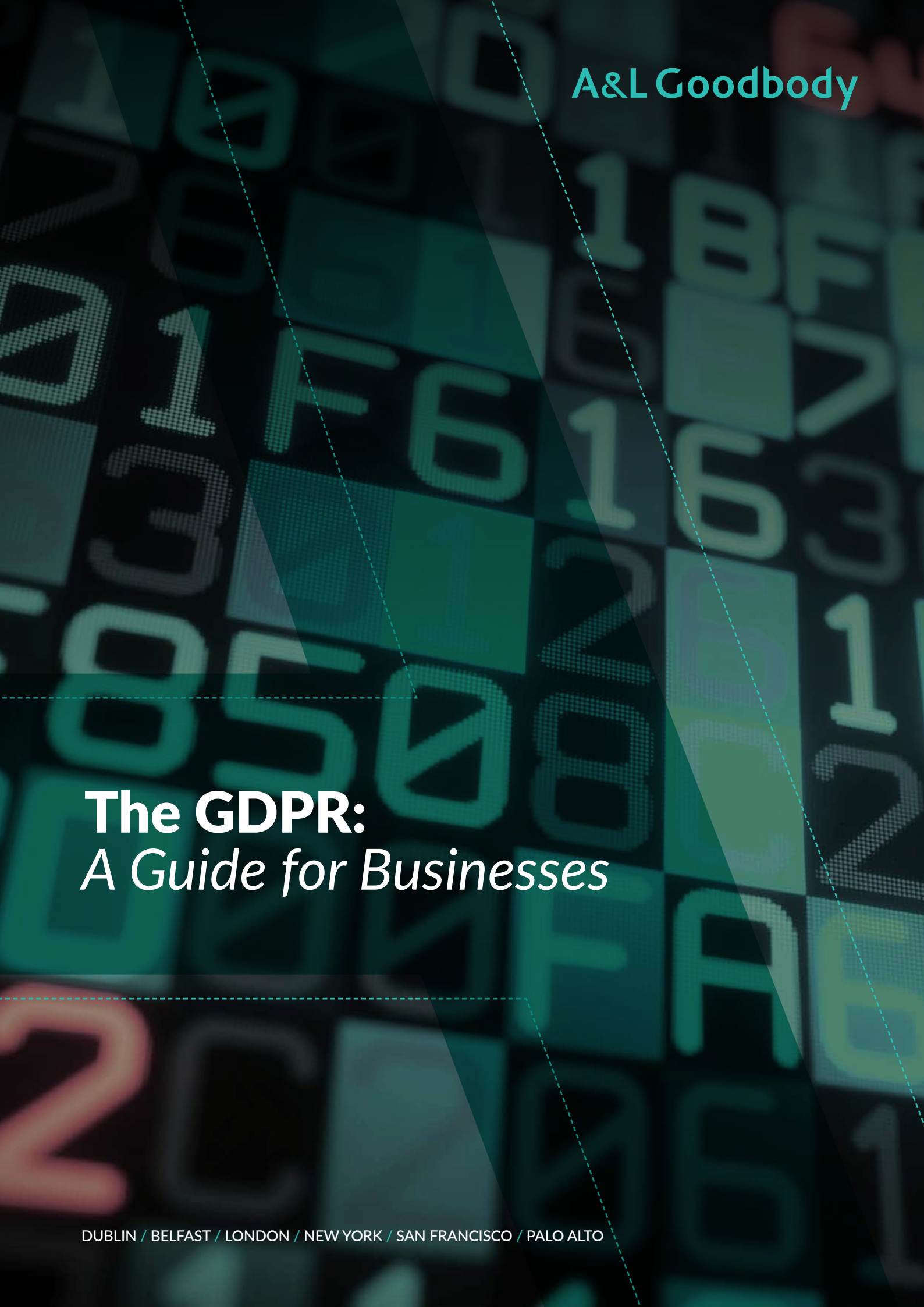

A&L Goodbody

The GDPR:
A Guide for Businesses

DUBLIN / BELFAST / LONDON / NEW YORK / SAN FRANCISCO / PALO ALTO

The GDPR:
A Guide for Businesses

Introduction

The EU General Data Protection Regulation (**GDPR**) was initially published in January 2012, and finally adopted on 27 April 2016. It will come into force on **25 May 2018**. The GDPR introduces substantial changes to data protection law. Given its extra-territorial scope, new concepts, (such as privacy by design and by default, and the concept of accountability), along with the severe financial penalties for non-compliance, businesses must start taking steps now to review and revise their policies and procedures as appropriate.

Existing data protection law is based on Directive 95/46/EC (**the Directive**) which was introduced in 1995, and had to be transposed into the national laws of each Member State. As a result of different interpretations of the Directive being applied by Member States, inconsistent data protection laws currently exist across the EU. In contrast, the GDPR is a directly-effective Regulation which will be immediately applicable across the EU from 25 May 2018, without the need for Member States to implement national legislation. It is likely, however, that the Irish Government will introduce legislation repealing the Data Protection Acts 1988 and 2003, which will provide, where permitted, for any national derogations from the GDPR.

The GDPR aims to make it easier for multinational companies operating across the EU to comply with data protection laws through the harmonisation of such laws. However, it permits Member States to legislate in many areas, which means that inconsistencies will still arise. It also aims to simplify regulation through the introduction of a 'one stop shop' whereby multinational companies will only have to deal with one supervisory authority, located in the Member State of their main establishment. But, the GDPR, as adopted, contains a significantly watered down version of the 'one stop shop' concept, which was originally proposed by the European Commission. As a result, supervisory authorities in other Member States can be involved in certain cases, and the lead authority must cooperate and endeavour to reach a consensus with other concerned authorities. In addition, the GDPR significantly increases the rights of individuals and the information to be given to them regarding processing activities.

This guide is intended to provide you with a **summary of some of the significant changes** that will apply once the GDPR comes into force and the **likely impact** of the GDPR on businesses. It also contains **priority action points** that businesses can begin taking to ensure compliance with the GDPR when it comes into force.

We will be happy to provide you with further information on any aspect of the GDPR on request.

Date of Publication: 19th February 2018

The GDPR:
A Guide for Businesses

INDEX

1 Extra-Territorial & Material Scope

At a glance

- The GDPR expands the territorial and material scope of EU data protection law.
- It applies to both controllers *and processors* established in the EU.
- It also captures controllers and processors *outside the EU*, who offer goods and services to, or monitor, EU residents. These businesses may need to appoint a representative in the EU.

Changes

(i) Extra-Territorial Scope

- The GDPR expands the territorial scope of the EU data protection law, capturing both controllers *and processors* in the EU, and those *outside the EU* who offer goods and services to, or monitor, EU residents.

EU established controllers and processors

- The GDPR applies to controllers and processors who have an EU *"establishment"* and process personal data *"in the context of activities"* of such an establishment, regardless of whether the actual data processing occurs within the EU or not (Article 3(1)).
- The GDPR does not define what constitutes an EU 'establishment', but the recitals state that it implies *"the effective and real exercise of activity through stable arrangements"*. The legal form of such arrangements, whether through a branch or subsidiary with a legal personality, is not the determining factor (Recital 22).
- The broad interpretation of *"establishment"* taken by the Court of Justice of the EU, in *Google Spain* (C-131/12) and *Weltimmo* (C-230/14) within the context of the Data Protection Directive 95/46/FC (the **Directive**) will likely continue to apply under the GDPR, leading to entities outside the EU being subject to the GDPR due to the activities of a separate legal entity in the EU.

Non-EU established controllers and processors who target or monitor EU data subjects

- The GDPR also applies to non-EU controllers and processors who process personal data of data subjects in the EU, where the processing relates to:
  - The offering of goods or services (irrespective of whether a payment is required); or
  - The monitoring of their behaviour (Article 3(2)).
- Non-EU data controllers and processors who offer goods and services to, or monitor EU residents must designate in writing a representative in the EU, unless subject to one of the specified exemptions in the GDPR (Article 27).
- The recitals provide that in order to ascertain whether a controller or processor outside the EU is *"offering goods or services"* to data subjects in the EU, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the EU. The mere accessibility of the website in the EU is insufficient to ascertain such intention. The possibility of ordering goods or services in the language or currency generally used in a Member State may however make it apparent that the controller envisages offering goods or services to data subjects in the EU (Recital 23).
- The recitals further provide that in order to determine whether a processing activity can be considered to *"monitor the behaviour of data subjects in the EU"*, it should be ascertained whether individuals are tracked on the internet to create profiles, in particular, in order to take decisions or analyse and predict personal preferences, behaviour and attitudes of individuals (Recital 24).

(ii) Material scope

- The GDPR applies to controllers and processors. It places new legal obligations on processors, with the result that they will be directly liable to data subjects for any damage caused by breaching the GDPR and subject to fines by the supervisory authority (Article 28-31).
- The GDPR applies to *"personal data"*. The definition in the GDPR is more detailed than the Directive, extending to an identification number, location data and online identifier, whilst sensitive personal data now includes genetic and biometric data (Article 4(1) & Article 9(1)).
- The right to the protection of personal data is *"not an absolute right"* and must be balanced against other fundamental rights, in accordance with the principle of proportionality, including freedom to conduct a business (Recital 4).

Exemptions

- The GDPR does not apply to the processing of personal data which (Article 2(2)):

WHERE TO FIND THIS
Articles 2-3 & 27-31
Recital 22-24

- » Falls outside the scope of EU law (e.g. national security);
- » Concerns EU common foreign and security policy;
- » Is by a natural person in the course of a purely personal or household activity. (This includes correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, the GDPR applies to controllers or processors which provide the means for processing personal data for such personal or household activities (Recital 18));
- » Is 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;
- » Is by EU institutions where Regulation (EC) No. 45/2001 (on the protection of individuals with regard to the processing of personal data by EU institutions and bodies and on the free movement of such data) applies instead. That Regulation will be adapted to ensure consistency with the GDPR (Article 2(3)); or
- » Concerns deceased persons (Recital 27).

E-Commerce Directive

- The GDPR will be *"without prejudice"* to the application of the E-Commerce Directive 2000/31/EC, in particular to the rules concerning the liability of intermediary service providers, which limit their liability where they act as a mere conduit, host, or cache (Article 2(4)). In regard to the interaction between the E-Commerce Directive and the GDPR, it seems, but is not expressly stated, that the E-Commerce Directive will determine the liability of ISPs for actions of users, whilst other obligations such as the rectification or erasure of data, will be governed by the GDPR.

E-Privacy Directive

- The GDPR exists in parallel with the e-Privacy Directive 2002/58/EC. The latter sets out the rules on electronic direct marketing and cookies. The GDPR does not impose any additional obligations in regard to the processing of personal data which is already subject to obligations set out in the e-Privacy Directive (Recital 173 & Article 95). Therefore the e-Privacy Directive continues to regulate electronic marketing. However, the e-Privacy Directive does adopt the definition of consent in the GDPR, with the result that the GDPR conditions for obtaining valid consent are applicable in situations falling within the scope of the e-Privacy Directive (WP29 Guidance on Consent). The European Commission has published a draft e-Privacy Regulation, which will replace the existing e-Privacy Directive, and ensure consistency with the higher standard of data protection provided by the GDPR.

Business Impact

- Controllers established within the EU are already subject to EU data protection law, but will need to comply with increased statutory obligations.
- Processors established in the EU will now be subject to the GDPR's direct statutory obligations for processors, rather than just the obligations imposed on them by contract by the controller, and will need to take steps to comply.
- Non-EU controllers and processors that process data of EU data subjects through websites and cookies will most likely come within the remit of the GDPR and will need to take steps to comply.

Action Points

- All controllers and processors established in the EU need to review their policies and procedures and amend them as appropriate to comply with the GDPR.
- All controllers and processors not established in the EU who target data subjects in the EU, by offering them goods or services, or monitoring their behaviour, need to review and revise their policies and procedures to ensure that they are in compliance with the GDPR. They may also need to appoint a representative within the EU who will act as a point of contact for supervisory authorities.

2 Definition of Personal & Sensitive Data

At a glance

- The GDPR broadens the definition of personal data and sensitive data.
- Personal data now expressly includes an identification number, location data, and online identifier. Sensitive personal data includes genetic data and biometric data.
- Data concerning criminal convictions is no longer classified as sensitive data, but it continues to benefit from special protection.
- Pseudonymisation is a privacy-enhancing technique where directly identifying data is held separately and securely from processed data to ensure non-attribution. Although pseudonymisation can reduce risks to the data subjects, it is not alone sufficient to exempt data from the scope of the GDPR.
- Anonymised data is not considered to be personal data.

WHERE TO FIND THIS
Articles 4, 9, 10,
Recitals 26 & 30

Changes

- The GDPR broadens the definition of personal data and sensitive data.
- The GDPR, like the Directive, defines *"personal data"* as *"any information relating to an identified or identifiable natural person"*. The GDPR further indicates that *"an identification number"*, *"location data"*, and *"online identifier"* (i.e. an IP address) constitute personal data where they can lead to identification of individuals (Recital 30 & Article 4(1)).
- The GDPR extends the definition of *"special categories of data"* (i.e. sensitive data) to include, in addition to data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life, "genetic data" and "biometric data".
- The GDPR provides definitions of *"biometric"* and *"genetic"* data. Practical examples of *"genetic data"* would be biological samples from an individual, such as chromosomal or DNA. Whilst *"biometric data"* should include fingerprints and facial recognition etc.
- The definition of sensitive data no longer includes information relating to criminal convictions, but such data continues to benefit from special protection (Article 10).
- As with the Directive, sensitive data is afforded more protection and requires more stringent conditions to be satisfied in order to legitimise its processing (Article 9).
- The GDPR introduces a new concept of *"pseudonymisation"*, which is defined as *"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 [such as encryption] and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"* (Article 4(5)).
- Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, constitutes personal data, within the scope of the GDPR. To determine whether a person is identifiable, account should be taken of all means reasonably likely to be used, (taking into account the cost, time and available technology) by the controller or another person to identify the individual directly or indirectly (Recital 26).
- However, pseudonymised data will be afforded certain relaxations from the requirements of the GDPR. For example, where data is pseudonymised and encrypted, a company will not be required in the case of a data breach to inform a data subject of the breach (Article 32(1)(a) & Article 34(3)(a)).

- Pseudonymisation is not the same as anonymisation. Anonymising data means processing it with the aim of irreversibly preventing the identification of the individual to whom it relates. Irreversibly anonymised data is not personal data, and therefore falls outside the scope of the GDPR (Recital 26).

Business Impact

- Many organisations, particularly those involved in data analytics, behavioural advertising, and social media will be affected by the express inclusion of online identifiers in the definition of *"personal data"*.
- The potential inclusion of pseudonymisation data within the scope of the GDPR will also affect organisations that rely on this technique to escape the application of EU data protection laws, such as hospitals carrying out clinical research. However, it would be prudent for organisations to apply pseudonymisation to personal data in order to meet their data protection obligations (e.g. data protection by design and security obligations) under the GDPR and, in particular, to reduce their potential liability to data subjects and/or the imposition of administrative fines. It may also permit organisations to process data further, for a purpose other than that for which it was collected, without a data subject's consent, as such processing will be deemed to be subject to appropriate safeguards (Article 6(4)(e)).

Action Points

- Companies engaged in monitoring of online behaviour through IP addresses or cookies; collecting genetic or biometric data; or applying pseudonymisation to data, should consider whether they are caught by the extended definition of personal data and sensitive data, and if so, review and amend their policies and procedures to ensure compliance with the GDPR.

3 Obligations on Processors

At a glance

- The GDPR contains a longer list of terms that *must* be included in data processing contracts.
- The GDPR imposes certain direct statutory obligations on data processors, meaning they will be subject to direct enforcement by supervisory authorities, fines and compensation claims by data subjects.
- The GDPR limits the liability of processors to the extent that they have not complied with their statutory obligations or have acted outside the instructions of the controller.

WHERE TO FIND THIS
Article 28-33, 37, 44 & 82-83, Recitals 81-82

Changes

- The GDPR imposes direct statutory obligations on data processors (e.g. outsourced service providers, private investigators) (Article 28 & 29). This means processors are subject to direct enforcement by supervisory authorities, serious fines, and direct liability to data subjects for any damage caused by breaching the GDPR (Articles 82 & 83).
- This is a significant change as the Directive merely requires processing to be governed by a written contract (including in electronic form), and that the processor shall carry out the processing solely on the instructions of the controller and take appropiate security measures. Despite the existence of such a contract, controllers currently remain legally responsible for any breaches of data protection law caused by the actions of their processors.
- **Direct statutory obligations imposed by the GDPR on processors include:**
  - Maintain records of data processing activities and make same available to the supervisory authority on request (Article 30);
  - Co-operate with the supervisory authority (Article 31);
  - Take appropriate security measures and inform controllers of any data breaches without undue delay (Articles 32 & 33);
  - In specified circumstances, designate a data protection officer (Article 37), and
  - Comply with restrictions regarding cross-border transfers (Article 44).
- The GDPR imposes more prescriptive obligations in regard to the terms of a data processing contract.
- **The written processing contract must set out:**
  - The subject matter and duration of the processing.
  - Nature and purpose of the processing.
  - Type of personal data.
  - Categories of data subjects and
  - Obligations and rights of the controller.
- **The GDPR requires the following mandatory terms to be imposed on a processor:**
  - To process data only on the documented instructions from the controller;
  - To ensure that the processor's staff are committed to confidentiality;
  - To take all appropriate security and organisational measures;
  - To sub-contract only with the prior written permission of the controller;
  - To pass onto the sub-processor the same data protection contractual obligations imposed on the processor;
  - To assist the controller in complying with the rights of data subjects;
  - To assist the controller in complying with its security and data breach notification obligations; conducting data protection impact assessment and prior consultation procedures;

- To delete or return all personal data to the controller, if requested, at the end of the processing; and
- To make available to the controller all information necessary to demonstrate compliance with its processing obligations and allow audits and inspections to be conducted by the controller and
- To inform the controller, if in its opinion, an instruction infringes the GDPR or EU or national data protection laws (Article 28(3)).

Liability

- The GDPR limits the liability of processors to a certain extent, by providing that they will only be liable for damage caused where they have not complied with processor-specific obligations in the GDPR or acted outside the instructions of the relevant controller (Article 82(2)).
- Where a controller or processor has paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controller or processor involved, that part of the compensation corresponding to their responsibility for the damage (Article 82(5)).
- If a processor infringes the GDPR by determining the purposes and means of processing, the processor will be considered to be a controller in respect of that processing (Article 28 (10)).

Business Impact

- The GDPR strikes a more even balance between data controllers and processors by making them jointly and severally liable according to their respective responsibility for the harm caused by a breach of data protection law.
- Although the Directive already requires data controllers to enter into written contracts with data processors, more protracted contractual negotiations are likely to occur between data controllers and processors going forward, in order to comply with the increased requirements set out in the GDPR regarding processing contracts, and to ensure appropriate risk allocation for data breaches between processors and controllers.

Action Points

- Businesses should carefully review and revise their data processing contracts to ensure that they meet the requirements of the GDPR and clearly specify the scope of the processor's responsibility. Any new data processing contracts should be agreed in accordance with the requirements of the GDPR.
- Mechanisms should be agreed for resolving disputes regarding respective liabilities to settle compensation claims, as there will inevitably be litigation on the issue of causation in the context of a data breach, in light of the new provision allowing for joint liability for data protection breaches.
- Processors will also need to review and revise their data breach, security and record-keeping policies and procedures etc. to meet their new statutory obligations under the GDPR.

4 Data Protection Principles & Accountability

At a glance

- The data protection principles remain largely the same. There are six general principles including: fairness; purpose limitation; data minimisation, accuracy; storage limitation, and security.
- The GDPR introduces a new concept of accountability, which requires controllers to be able to demonstrate how they comply with the data protection principles.
- Records of processing activities must be kept by controllers, and supplied to supervisory authorities on request, to demonstrate their compliance with the GDPR.

WHERE TO FIND THIS
Article 5, 15, 24 & 30, Recital 39 & 82

Changes

- The data controller remains responsible for ensuring compliance with the data protection principles. The principles in the GDPR remain largely the same as those in the Directive, but contain some new elements, as highlighted in italics below (Article 5(1)):
  - **Lawful, fair and transparent processing** – Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;
  - **Purpose limitation** – Personal data must be processed for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes. *Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes* (subject to the conditions in Article 89(1), concerning implementation of appropiate technical and organisational measures.
  - **Data minimisation** – Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
  - **Accuracy** – Personal data must be accurate, and where necessary kept up to date; *every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;*
  - **Storage limitation** – Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. *Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes* (subject to the implementation of appropriate technical and organisational measures in accordance with Article 89(1));
  - **Security, 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.
- The principle concerning right of access remains in substance but no longer in the form of a principle (Article 15).
- The GDPR also introduces **a new concept of accountability**, which requires controllers to be able to demonstrate how they comply with the data protection principles (Article 5(2)).
- The requirement to demonstrate compliance runs through the core of

the GDPR. For example, controllers must be able to demonstrate that consent was given (Article 7); that appropriate technological and organisational measures are in place to ensure that processing is conducted in compliance with the GDPR (Article 24); that there are compelling legitimate grounds for the processing when a data subject objects to such processing (Article 21).

- Controllers can demonstrate compliance with the GDPR by:
  - » Implementing a data protection policy (Article 24(2)) and
  - » Adhering to approved codes of conduct or approved certification mechanisms (Article 24(3)).
- It is mandatory for controllers and processors to maintain records of processing activities and to make them available to the supervisory authority on request. Only organisations with less than 250 employees are exempt from this obligation (unless the processing carried out is likely to result in a risk to the rights of data subjects, the processing is not occasional, or the processing includes sensitive data or data relating to criminal convictions) (Article 30(5)).
- Records to be retained by controllers include (Article 30(1)):
  - » The name and contact details of the controller; any joint controller; the controller's representative; and the data protection officer;
  - » The purposes of such processing;
  - » The categories of data subjects; recipients; and personal data processed;
  - » The time limits for erasure of data;
  - » Details of non-EEA data transfers and safeguards in place; and
  - » A description of the technical and organisational security measures in place.
- Processors are required to retain similar records (Article 30(2)).

Business Impact

- Due to the new concept of accountability and record-keeping obligations in the GDPR, businesses will no longer have to register or notify supervisory authorities on their processing activities. Instead, data controllers will have to implement appropriate technical organisational measures to demonstrate that their data processing is performed in accordance with the GDPR.
- The concept of accountability has been the discussion of supervisory authorities both in the EU and globally for some time. In 2010, the Article 29 Working Party (**WP29**) issued an Opinion 3/2010 putting forward a proposal for a principle on accountability with the aim of moving the protection of data from '*theory to practice*' as well as helping data protection authorities in their supervision and enforcement tasks. The principle of accountability was also expressly recognised by the Organisation for Economic Cooperation and Development's (**OECD**) privacy guidelines adopted in 1980.

Action Points

- In order to comply with the new record keeping requirements, businesses should review their data processing activities, and retain records of the results and any actions taken to address any gaps. Businesses should be aware that these records will be required to be made available to supervisory authorities on request, to demonstrate how they comply with the GDPR.
- As the GDPR expressly recognises the implementation of appropriate data protection policies as a method for controllers to demonstrate their compliance with the GDPR, businesses should review their data protection policies, and ensure they set out the full details of their processing activities to meet the increased information rights of individuals under the GDPR.
- Businesses should further consider making binding and enforceable commitments, via contractual or other legally binding instruments, to adhere to approved codes of practice or certification mechanisms, as the GDPR also recognises such adherence as demonstrating compliance.

5 Lawful Processing Conditions, including Consent, Legitimate Interests & Further Processing

At a glance

- The grounds for processing personal data remain largely the same.
- Consent will become more difficult to rely on to legitimise processing.
- The GDPR blurs the distinction between consent and explicit consent, as both require some form of clear affirmative action. Silence or pre-ticked boxes will no longer be sufficient to constitute consent.
- The GDPR permits data subjects to withdraw their consent at any time.
- There is a higher bar for relying on *"legitimate interests"* and an indication of when it may be used. Public authorities cannot rely on *"legitimate interests"* to legitimise their processing.
- The GDPR contains a non-exhaustive list of factors to be taken into account when determining whether further processing is compatible with the purpose for which the data were collected.

Changes

Lawful Processing Conditions

- In addition to complying with the six data protection principles (see section 4), a controller must have a legal basis to process personal data (also known as "lawful processing conditions").
- While remaining largely the same, there are some changes to the legal bases for processing personal data and sensitive personal data.
- The table below sets out the legal bases for processing personal data, and the impact of the GDPR (Article 6).

Legal bases for processing	Impact of GDPR
Consent of the data subject	New limitations on the use of consent to legitimise processing
Necessary for the performance of a contract with the data subject or to enter into such a contract	No change
Necessary for compliance with a legal obligation to which the controller is subject	Clarifies that the legal obligation must be laid down by EU or Member State law to which the controller is subject, and does not necessarily require a legislative act, thus common law should suffice
Necessary to protect the vital interests of the data subject or another natural person	No change
Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	Clarifies that the task carried out or official authority vested in the controller should have a basis in EU or Member State law
Necessary for the purposes of the legitimate interests of the controller or a third party except where such interests are overridden by the interests of a data subject, in particular where the data subject is a child	The requirement to consider the specific interests of children is new. Public authorities can no longer rely on legitimate interests to legitimise data processing carried out in the discharge of their functions

WHERE TO FIND THIS
Article 4, 6-9,
Recitals 32, 38, 40-50, 171
WP29 Guidance on Consent

The table below sets out the legal bases for processing sensitive personal data, and the impact of the GDPR (Article 9).

Legal bases for processing	Impact of GDPR
Explicit consent	No change
Necessary for compliance with employment, social security or social protection legal obligations, or a collective agreement	Extended to include compliance with social security and social protection legal obligations. Clarifies that the legal obligation must be based on EU or Member State law
Necessary to protect the vital interest of a data subject or any natural person who is physically or legally incapable of giving consent	No change
Processing by not-for-profit bodies or associations with philosophical, political, religious or trade union aims, in relation to members or former members, or persons in regular contract with it	Clarifies that the processing may also concern "former members" of the body in question
Personal data manifestly made public	No change
Necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity	Clarifies that this ground covers processing of personal data by courts acting in their judicial capacity
Necessary for substantial public interest reasons on the basis of EU or Member State law	Introduces a proportionality requirement
Necessary for the purposes of preventative or occupational medicine, on the basis of EU or Member State law	Covers a wider range of activities, including social care, occupational medicine and assessing the working capacity of an employee. It also clarifies that the activity in question must be on the basis of EU or Member State law, or pursuant to a contract with a health professional
Necessary for public health reasons	A new ground, including a broad definition of "public health" (Recital 54)
Necessary for archiving, scientific or historical research, or statistical purposes based on EU or Member State law	A new ground

Consent - An analysis

- The GDPR introduces a higher bar for relying on consent. Like the Directive, the GDPR refers to *"consent"* and *"explicit consent"*. However, the difference between the two is less clear, as both now require some form of clear affirmative action. Thus silence, pre-ticked boxes or inactivity will not be sufficient to constitute consent.
- The GDPR defines *"consent"* as *"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"* (Article 4(11)).
- The recitals highlight that such affirmative action could include *"ticking a box when visiting an internet website, or choosing technical settings for information society services"* (Recital 32).
- The GDPR contains a list of conditions for valid consent, including:
  - Consent must be verifiable (i.e. some form of record must be kept of how and when consent was given) (Article 7(1));
  - Where consent is given in a written declaration which also concerns other matters (e.g. a contract), the request for consent must be clearly distinguishable from the other matters (Article 7(2));
  - Prior to giving consent, data subjects must be informed of their right to withdraw consent at any time and it must be easy for them to do so (i.e. allowing consent to be withdrawn in the same media in which it was obtained, such as via a website or email) (Article 7(3)); and
  - When assessing if consent has been freely given *"utmost account"* must be taken of the fact that the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract (i.e. such consent is unlikely to be considered to be freely given) (Article 7(4)).
- The controller bears the burden of proving that the data subject has validly consented to the processing of his/her data (Article 7 (1)).
- The recitals to the GDPR highlight that a declaration of consent pre-formulated by the controller should not contain unfair terms. Consent will not be regarded as freely given if the data subject has no genuine or free choice or cannot refuse or withdraw consent without detriment (Recital 42).
- Consent will not always be the best mechanism to legitimise processing, and controllers should take time to consider whether another ground is more appropriate (WP29 Guidance).
- If a controller finds that current consents do not meet the standard of GDPR consent, then controllers will need to obtain fresh consents, or assess whether processing may be based on a different legal basis. However, this is a one-off situation, as under the GDPR it is not possible to swap between one legal basis and another (WP29 Guidance).
- The GDPR continues to require *"explicit"* consent for the processing of sensitive data, but does not specify what action constitutes *"explicit"* consent (Article 9(2) (a)). However the WP29 clarifies that *"explicit"* means that the data subject must give an express statement of his or her consent.
- Examples of *"explicit"* consent include written and signed statements, electronic signatures, filling in an electronic form, sending an email, uploading a scanned signature or a recorded oral statement.
- The GDPR includes more stringent conditions for information society services (e.g. online businesses) to rely on consent to process children's data (Article 8). It requires such service providers to obtain, and make reasonable efforts to verify parental consent to the processing of a child's data, where the child is below the age of 16 years old. Member States may provide by law for a lower age, so long as that age is not below 13 years old. The introduction of this age limit will not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child (Article 8(3)).
- The GDPR does not prescribe a specific time limit for how long consent lasts, but best practice is to refresh consent at appropriate intervals (WP29 Guidance).

Legitimate Interests - An analysis

- Where legitimate interests are relied on as a legal basis for processing (non-sensitive) data, the data subject, at the time when personal data is obtained, must be informed of the legitimate interests pursued by the controller or by a third party (Article 13(1)(d) & Article 14(2)(b)).
- The recitals note that *"the existence of a legitimate interest would need*

careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place" (Recital 47).

- The recitals highlight that processing of personal data could be necessary for the legitimate interest of a controller where it is necessary:
  - For the purposes of preventing fraud (Recital 47);
  - For direct marketing purposes (Recital 47);
  - For the transmission of personal data within a group of undertakings for internal administrative purposes, including the processing of client and employee data (Recital 48);
  - For the purposes of ensuring security (Recital 49); or
  - For reporting possible criminal acts or threats to a competent authority (Recital 50).
- The GDPR contains a new provision allowing data transfers out of the EEA on the basis that it is necessary for the legitimate interests of the controller, subject to certain conditions (Article 49(1)).

Further Processing - An analysis

- The GDPR contains a non-exhaustive list of the factors to be taken into account to ascertain whether further processing (which is not based on consent or an EU or Member State law) is compatible with the purpose for which the personal data was initially collected (Article 6(4)), including:
  - Any link between the original purpose and the further processing purpose;
  - The context in which the personal data was collected, in particular the relationship between the data subjects and the controller;
  - The nature of the personal data, in particular whether sensitive or criminal data are processed;
  - The possible consequences of the further processing for data subjects;
  - The existence of appropriate safeguards, including encryption or pseudonymisation.

Business Impact

- Businesses will have to explain the legal basis for processing personal data in their privacy notices and when they respond to a data access request.
- The difference between what constitutes consent and explicit consent is not clear and we await further guidance on this issue. However, it is evident that there will need to be a positive indication of consent to personal data being processed. Consent cannot be inferred from silence, pre-ticked boxes or inactivity.
- The GDPR requires businesses to be able to demonstrate that consent has been given, and procedures must be in place for recording consent. Businesses should also be aware that individuals shall have a stronger right to have their data deleted where consent is relied on as a legal basis for processing.

Action Points

- Businesses should review the types of data processing they are carrying out, and be clear about their legal basis for carrying it out, and document it.
- Businesses should review how they are obtaining and recording consent and whether any changes are needed. Data subjects must be given a genuine and granular choice as to whether to consent. If consent is given it should be capable of being easily withdrawn. In particular, businesses offering online services to children should consider how to obtain parental consent and verification of such consent. Records of actual consent given should be maintained.
- Given the heightened consent requirements, businesses should consider using consent as a legal basis only as a last resort. If consent is withdrawn, controllers cannot swap to another legal basis.
- If personal data that is not necessary for the performance of the contract is processed on the basis of consent (e.g. profiling) it would be prudent to ensure that privacy notices clearly identify this and allow the data subject to easily refuse to provide consent.
- If relying on legitimate interests to justify data processing, a record of the assessment made in relation to the balance of interests of the controller or third party and the rights of data subjects should be documented, and included in the privacy notice supplied to data subjects.

6 Privacy Notices

At a glance

- The GDPR provides a list of specific, additional, information that must be provided to data subjects to ensure all processing activities are transparent.
- This list includes, in particular, the legal basis for the processing and the data retention period or criteria used to determine same.

Changes

- Transparency is an overarching obligation under the GDPR. The information requirements are outlined in Articles 12-14 of the GDPR.
- The GDPR sets out the minimum information that must be supplied to data subjects in order to comply with the principle of fair, lawful and transparent processing.
- The objective of the transparency principle is that it should be transparent to natural persons how their personal data is collected, used, consulted or otherwise processed, and to what extent it is processed (Recital 39).
- Controllers must also update privacy notices concerning processing that is already underway, to ensure they are compliant with the GDPR transparency obligations. This means that prior to 25 May 2018, controllers must revisit all information provided to data subjects on processing of their personal data to ensure they adhere to the requirements in relation to transparency (Recital 171 & WP29 Guidance).

WHERE TO FIND THIS
Article 12-14,
Recitals 58-62
WP29 Guidance on Transparency

Format of Notice

- The controller must take steps to provide the requisite information to data subjects in:
  - a concise, transparent, intelligible and easily accessible form
  - using clear and plain language
  - in writing, or by other means, including, where appropriate, by electronic means, or
  - where requested by the data subject it may be provided orally (Article 12(1)).
- The requirement to provide the requisite information in a *"concise and transparent"* manner means that controllers should present the information succinctly in order to avoid information fatigue (WP29 Guidance).
- *"Intelligible"* means that it should be understood by an average member of the intended audience (WP29 Guidance).
- *"Easily accessible"* means that the data subject should not have to seek out the privacy notice; it should be immediately apparent to them where this information can be accessed, for example by providing it directly to them or by linking them to it (WP29 Guidance).
- The requirement for *"clear and plain language"* means the information should be provided in as simple a manner as possible. The information should be concrete and definitive, and not phrased in ambivalent terms, leaving room for different interpretations. Language qualifiers such as "may" or "might" should be avoided. An example of unclear language is: *"We may use your personal data to develop new services"*, as it is unclear what the services are, or how the personal data might develop them (WP29 Guidance).
- The information may be provided by a variety of methods, including in writing, orally or electronically through layered privacy notices; privacy dashboards; "just-in-time" pop-ups; hover-over notices, or videos.
- The information may be provided to data subjects *"in combination"* with standardised icons, to enhance transparency, and reduce the need for vast amounts of written information to be presented to data subjects. The GDPR assigns responsibility for the development of a code of icons to the European Commission (Article 12(7), 12 (8) & Recital 166).

Information to be provided to data subjects

- Pursuant to Article 13 of the GDPR, where the controller **obtains the personal data directly** from the data subject, the following information must be supplied by the controller, at the time when personal data are obtained:
  - The identity and contact details of the controller or its representative;
  - The contact details of the data protection officer, where applicable;
  - The purpose of the processing and the legal basis for the processing;
  - The legitimate interests of the controller or a third party

and an explanation of those interests (where processing is based on this ground);

- The recipients or categories of recipients of the personal data;
- Details of any transfers out of the EEA, safeguards in place and the means by which to obtain a copy of them;
- The data retention period or criteria used to determine same;
- The individual's rights, including the right of access to data; rectification and erasure; restriction of the processing; objection to processing and to data portability;
- Where the processing is based on consent, the right to withdraw it at any time;
- The right to complain to the supervisory authority;
- Details of automated decision-making, including profiling and logic involved, as well as the significance and consequences of such processing for the data subject, and
- Whether the provision of personal data is a statutory or contractual requirement or obligation, and the consequences of failure to provide such data.

- Pursuant to Article 14 of the GDPR, where the controller **does not obtain the data directly** it must, within one month, provide the data subject with similar information to that listed above, and in addition, the categories of data processed; from which source the data originated; and, if applicable, whether it came from publicly accessible sources (Article 14).
- Where the controller intends to further process the data other than for the purpose for which it was collected, the controller must inform the data subject, prior to the further processing, of that other purpose (Article 13(3) & 14(4)).

Business Impact

- Businesses will need to provide individuals with more detailed information in their privacy notices concerning how they process personal data. All processing activities will need to be transparent. Businesses may find it challenging deciding which processing grounds they will rely on to legitimise the processing of personal and sensitive data, and the applicable retention periods. It is likely that a large amount of preparatory work will be required to establish this information before it can be translated into privacy notices.

Action Points

- All privacy notices and/or policies will need to be reviewed and revised to comply with the additional information requirements and ensure that processing is fair and transparent.

Exemptions

- Article 13(4) contains one exemption to a controller's obligation to provide certain information to data subjects, where it has obtained their personal data directly. That exemption applies *"where and insofar as the data subject already has the information"*. The WP29 states that this exemption should be construed narrowly, and the phrase *"insofar as"* makes it clear that even if a data subject has previously been provided with certain categories from the inventory of information set out in Article 13, there is still an obligation on the controller to supplement that information in order to ensure that the data subject now has a complete set of the information required.
- Article 14(5) contains four exemptions to a controller's obligation to provide certain information to data subjects, where it has indirectly obtained their personal data. These exemptions apply where:
  - The data subject already has the information;
  - The provision of the information proves impossible, or would involve disproportionate effort, or would seriously impair the achievement of the objectives of the processing (in such cases the controller may make the information publicly available);
  - Obtaining or disclosure is expressly laid down by EU or Member State law to which the controller is subject; or
  - Where the personal data must remain confidential pursuant to an obligation of professional secrecy under EU or Member State law, including a statutory obligation of secrecy.

7 Subject Access Requests

At a glance

- The GDPR requires the provision of specific, additional, information to data subjects when responding to access requests.
- The time period for dealing with requests has been reduced from 40 days to 1 month.
- A data subject access request can only be refused where it is *"manifestly unfounded or excessive, in particular because of its repetitive character."*

WHERE TO FIND THIS
Article 12, 15 & 23, Recital 63

Changes

- The GDPR increases the amount of information to be given by a controller to a data subject when providing access.

Extent of Right of Access

- Individuals have a right to request access to a copy of their personal data. When providing such access, controllers must also provide the information listed below. The words in italics indicate the new information to be supplied under the GDPR (Article 15(1)):
  - The purposes of the processing;
  - The categories of personal data;
  - The recipients or categories of recipients;
  - *The data retention period or criteria used to determine that period;*
  - *The individual's rights including: the right to rectification, erasure; restriction or objection to the processing;*
  - *The right to complain to the supervisory authority;*
  - The source of the information if not collected directly from the data subject;
  - Details of any automated processing, including profiling; the logic involved, *and the significance and envisaged consequences of the processing for the data subject;* and
  - *Where data are transferred out of the EEA, the appropriate safeguards (Article 15(2)).*
- Where a controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered the data subject specify the information to which the request relates (Recital 63).

Exemptions

- A data subject access request may be refused only where the request is *"manifestly unfounded or excessive, in particular because it's repetitive character."* The controller will bear the burden of demonstrating the manifestly unfounded or excessive character of the request (Article 12(5)).
- However, the GDPR gives Member States discretion to restrict, by way of legislative measure, the scope of individuals' rights, including the right of access, where such restriction is necessary and proportionate to safeguard:
  - National security;
  - Defence;
  - Public security;
  - Prevention, investigation or prosecution of criminal offences;
  - Public interest objectives of EU or Member State law;
  - Protection of judicial proceedings;
  - Prevention, investigation or prosecution of breaches of ethics;
  - Regulatory function connected with the exercise of official authority;
  - The protection of the data subject; or
  - The enforcement of civil law claims (Article 23).

- The right of access should not adversely affect the rights of others (Article 15 (4)). This might cover the protection of trade secrets or intellectual property (Recital 63).

Time Limits, Fees & Format of Response

- The time period for dealing with requests has been reduced from 40 days to one month. The one month period may be extended by two further months where requests are complex or numerous. The controller must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay (Article 12(3)).
- The ability to charge a fee has also been removed. However, the controller may charge a reasonable fee for any further copies requested by the data subject, or where access requests are manifestly unfounded or excessive, taking into account the administrative costs of providing the information (Article 15(3) and 12(5)).
- Where a controller refuses to respond to a request, he/she must, without delay, and at the latest within one month explain why, informing the data subject of their right to complain to the supervisory authority and to a judicial remedy (Article 12(4)).
- The information must be provided in writing or by other means, including electronic means, when requested by the data subject (Article 12(1) & Article 15(3)).
- The information may also be provided orally, when requested by the data subject, provided that the identity of the data subject is proven by other means (Article 12(1)).
- The Recitals suggest that, where possible, a controller should provide remote access to a secure self-service system which would provide the data subject with direct access to his or her personal data (Recital 63).

Business Impact

- Businesses should be aware that there will likely be an increase in access requests, and there may be a need for increased administrative resources to deal with same. Businesses will be obliged to respond to access requests within one month unless they are *"manifestly unfounded or excessive"* or a national legislative measure allows access to be refused.

Action Points

- Procedures for handling data access requests will need to be reviewed and updated to provide the additional information which data subjects are entitled, and the more limited time period to respond.

8 Right to Rectification, Erasure, Restriction, Data Portability, Objection & Profiling

At a glance

- The GDPR provides data subjects with new rights, including a right to data portability, and a right not to be subject to a decision based on automated processing, including profiling, in certain circumstances.
- It gives data subjects more control by enabling them to object to processing which is based on the legitimate interests of the controller or a third party (including profiling based on that ground).

WHERE TO FIND THIS
Articles 4 (4), 12, 16-22, Recitals 65-68, 71 & 72
WP29 Guidance on Profiling
WP29 Guidance on Data Portability

Changes

(i) Right to Rectification

- Individuals have a right, similar to that under the Directive, to have personal data rectified if it is inaccurate or incomplete (Article 16).
- Where a data subject has requested the rectification of his/her personal data, the controller must inform recipients to whom that data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller must also inform the data subject about the recipients to whom the data has been disclosed, if he/she requests it (Article 19).
- A controller must provide information on action taken on a request for rectification to the data subject without undue delay, and at the latest within one month of receipt of the request. This period may be extended by two further months where requests are numerous or complex (Article 12(3)).

(ii) Right to Erasure

- Data subjects have the right to erasure, also known as 'the right to be forgotten'. Under the Directive, data subjects have a right to seek erasure of their data only where it is being processed other than in compliance with the data protection principles, in particular because of the incomplete or inaccurate nature of the data.
- The GDPR provides individuals with a broader right to have their data erased. Individuals will have a right to erasure in six scenarios:
  - » Where the personal data is no longer necessary in relation to the purposes for which it was collected;
  - » When the data subject withdraws his/her consent and there is no other legal ground for the processing;
  - » When the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
  - » The personal data have been unlawfully processed;
  - » The personal data have to be erased to comply with an EU or Member State legal obligation; or
  - » The personal data have been collected in relation to the offer of information society services to a child (Article 17(1)).
- Where the controller has made the personal data public, it must take *"reasonable steps"* to inform third party controllers who are processing it to erase any links to, copies or replications of the personal data in question. Such *"reasonable steps"* must take into account available technology and the cost of implementation (Recital 66 & Article 17(2)).
- A request for erasure of personal data can be refused where processing is necessary:
  - » For exercising the right to freedom of expression and information;
  - » For compliance with an EU or Member State legal obligation; or for performance of a public interest task or exercise of official authority;

- » For public health reasons;
- » For archiving interests in the public interest, scientific or historical research purposes or statistical purposes (insofar as the right to erasure is likely to render impossible or impair the achievement of those objectives); or
- » For the exercise or defence of legal claims (Article 17(3)).

- Where a data subject has requested the erasure of his/her personal data, the controller must inform recipients to whom that data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller must also inform the data subject about those recipients if he/she requests it (Article 19).

- A controller must provide information on action taken on a request for erasure to the data subject without undue delay, and at the latest within one month of receipt of the request. This period may be extended by two further months where requests are numerous or complex (Article 12(3)).

(iii) Right to Restriction of processing

- The GDPR introduces a new right to restriction of processing. This right replaces the right to blocking in the Directive. In certain circumstances it is an alternative to requiring the data to be erased.

- When processing is restricted, a controller is permitted to store the personal data, but not further process it (Article 18(2)).

- A data subject's right to restrict processing arises in four scenarios:
  - » Where the data subject contests the accuracy of the data, the processing should be restricted for a period enabling the controller to verify its accuracy;
  - » Where the processing is unlawful and the data subject opposes erasure and requests restriction instead;
  - » Where the controller no longer needs the personal data, but the data subject requires the data to exercise or defend a legal claim; or
  - » Where the data subject has objected to the processing, it should be restricted pending verification of whether the legitimate interests of the controller override those of the data subject (Article 18(1)).

- Methods by which to restrict the processing of personal data include, inter alia, temporarily moving the selected data to another processing system, making the selected data unavailable to other users, or temporarily removing the published data from a website. In automated filing systems, the restriction of processing should, in principle, be ensured by technical means in such a manner that the data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system (Recital 67).

- When a data subject exercises his/her right to restrict processing, the controller can only continue to process the data if:
  - » 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 (under EU or Member State law) (Article 18(2)).

- Where a data subject has requested the restriction of the processing of his/her personal data, the controller has an obligation to inform recipients to whom that data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller must also inform the data subject about those recipients if he/she requests it (Article 19).

- The controller must notify the data subject before lifting a restriction (Article 18(3)).

- A controller must provide information on action taken on a request for restriction of processing to the data subject without undue delay, and at the latest within one month of receipt of the request. This period may be extended by two further months where requests are numerous or complex (Article 12(3)).

(iv) Data Portability

- The new right to data portability enables individuals to obtain their data, and have their data transmitted to another controller without hindrance, where technically feasible. The WP29 Guidance on Data Portability provides examples of such hindrances, including fees asked for

delivering data, lack of access to a data format or API, or excessive delay or complexity to retrieve the full dataset.

- The right applies to personal data an individual has provided to a controller (e.g. mailing address, age) and to data generated by an individual's activity (e.g. a person's search history, traffic and location data). It does not extend to data generated by the controller (e.g. a credit score created by a bank) (Article 20(1) & (2)).
- The right to data portability only applies where:
  - » The processing is based on the data subject's consent (or explicit consent for sensitive data) or for the performance of a contract; and
  - » The processing is carried out by automated means (Recital 68 & Article 20(1)).
- 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 (Article 20(3)).
- The right to data portability must not adversely affect the rights and freedoms of others (including businesses).
- A controller must provide information on action taken on a request for data portability to the data subject without undue delay, and at the latest within one month of receipt of the request. This period may be extended by two further months where requests are numerous or complex (Article 12(3)).
- Data portability does not automatically trigger the erasure of the data from the controller's systems, and does not affect the original retention period applying to the data which have been transmitted (Article 17 and WP29 Guidance).

(v) Right to object to processing

- The GDPR broadens the current rights of data subjects to object to processing of their data. Under the Directive, data subjects have the right to object to the processing of data only where it causes unwarranted substantial damage or distress or it is used for direct marketing purposes.
- The GDPR does not provide a general right for a data subject to object to processing. Data subjects have a right to object to:
  - » Processing based on public interest or legitimate interest grounds (including profiling based on those grounds);
  - » Direct marketing (including profiling to the extent that it is related to such marketing); and
  - » Processing for scientific, historical research or statistical purposes (unless the processing is necessary for the performance of a public interest task) (Article 21).
- When a data subject objects to such processing, the controller must stop processing the personal data, unless the controller 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 (Article 21(1)).
- There are no grounds to refuse to comply with a data subject's objection to processing for direct marketing purposes (Article 21(3)).
- The right to object must be explicitly brought to the attention of the data subject, at the latest at the time of first communication with him/her, and must be presented clearly and separately from other information (Article 21(4)).
- A controller must provide information to the data subject on action taken on an objection to processing without undue delay, and at the latest within one month of receipt of the request. This period may be extended by two further months where requests are numerous or complex (Article 12(3)).

(vi) Automated decision-making and profiling

- The GDPR prohibits decisions based solely on automated processing, including profiling, which produce a legal effect or similar significant effect on an individual (Article 22 (1)).
- The words *"based solely"* mean the prohibition only applies where there is no human involvement in the decision process.
- The WP29 Guidance on Profiling acknowledges that it is difficult to be precise about what amounts to a sufficiently *"significant effect"* to meet the threshold. A typical example is automated refusal of an online credit application (Recital 71).
- Profiling *per se*, which does not result in solely automated decisions is not prohibited.
- The GDPR contains a new, broad, definition of profiling which is

defined as *"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 or behaviour, location or movements"* (Article 4(4)).

- The prohibition on decisions based solely on automated processing, including profiling, does not apply if the decision is:
  - » Necessary for the performance of a contract between the data subject and controller;
  - » Authorised by EU or Member State law (e.g. for the purposes of fraud or tax evasion); or
  - » Based on the explicit consent of the data subject (Article 22(2)).
- Where a decision based solely on automated processing, including profiling, occurs on the basis that it is necessary for the performance of a contract or with the explicit consent of the data subject, the data subject must be given *"at least the right"* to express his/her point of view and to contest the decision (Article 22(3)).
- Automated decision-making involving sensitive data is only allowed where the data subject has given his or her explicit consent or it is necessary for public interest reasons (Article 22 (4)).
- Controllers must inform data subjects, at the time personal data is obtained, of the existence of the automated decision-making, including profiling, and the logic (i.e. purpose) involved, as well as the significance and consequences of such processing for the data subject (Article 13(2) & 15(1)(h)).
- When processing personal data for profiling purposes, a controller must ensure that appropriate safeguards are in place (Recitals 71 & 72).
- A controller must provide information on action taken on a data subject's request not to be subject to a decision based on profiling without undue delay, and at the latest within one month of receipt of the request. This period may be extended by two further months where requests are numerous or complex (Article 12(3)).

Business Impact

- The GDPR provides individuals with increased rights, and more transparency, particularly in regard to profiling. It also gives data subjects more control by, for example, allowing them to object to profiling which is based on legitimate interest grounds or used for direct marketing purposes, and to have their profile erased, where there are no overriding legitimate grounds for the processing.

Action Points

- Companies should review and revise their privacy notices/policies and procedures in order to meet the new rights of individuals, and ensure that staff know how to respond to requests for rectification; erasure; data portability; restriction of processing requests or objections to the processing. In particular, companies will need to ensure appropriate IT systems are in place to deal with the right to erasure, restriction of processing and data portability.
- Companies will also need to review all profiling activities and ensure appropiate mechanisms are in place to obtain data subjects' consent to such activities.
- In addition, companies will have to ensure that staff are aware of their obligation to notify third party recipients of data requests for rectification, erasure or restriction of processing, and also the data subject about those recipients if he/she requests it. This notification obligation is likely to be difficult to meet where the data have been made public.

9 Data Privacy by Design, by Default and Data Privacy Impact Assessments (DPIAs)

At a glance

- The GDPR aims to establish a culture of privacy by design and default by requiring data privacy to be embedded into a business.
- DPIAs are a useful tool to help businesses to identify and address non-compliance risks. A DPIA will be compulsory where the proposed processing activities are likely to result in a *"high risk"* to data subjects, taking into account their nature, scope, and context.

WHERE TO FIND THIS
Article 25, 35 & 36,
Recitals 78, 84, 89-96
WP29 Guidance on DPIAs

Changes

Data Protection by Design & By default

- The GDPR introduces the concepts of *privacy by design* and *by default*, with the aim of organisations embedding data privacy into their operational processes and ensuring that data protection is no longer an after-thought (Article 25).
- ***'Privacy by design'*** requires data controllers to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement the data protection principles (such as data minimisation), in an effective manner.
- When deciding what technical and organisational measures are appropriate, businesses are required to take into account:
  - The state of the art;
  - The cost of implementation;
  - The nature, scope, context and purposes of the processing; and
  - The risks of the processing to individuals' rights (Article 25(1)).
- ***'Privacy by default'*** requires controllers to implement appropriate technical and organisational measures to ensure that, by default, personal data are processed only for the specific purpose for which they have been obtained, and are not made available or accessible to an indefinite number of individuals.
- The privacy by default obligation applies to:
  - The amount of personal data collected;
  - The extent of their processing;
  - The retention period; and
  - Accessibility (Article 25(2)).
- An approved certification mechanism may be used to demonstrate compliance with the requirements of privacy by design and by default (Article 25(3)).
- The recitals highlight that when developing, designing, selecting and using applications, services and products that are based on the processing of personal data, producers should be encouraged to take into account the right to data protection and, with due regard to state of the art, make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and default should also be taken into consideration in the context of public tenders (Recital 78).

Privacy Impact Assessments (DPIAs)

- DPIAs assist businesses to identify data privacy problems at an early stage, and address those problems in order to comply with data protection laws.
- DPIAs are compulsory under the GDPR, where the proposed processing activities are likely to result in a *"high risk"* to the rights of individuals, taking into account the nature, scope, context and purposes of the processing. Such processing activities may be those which, in particular, involve new technologies (Article 35 (1); Recitals 89 and 91).
- The precise meaning of "*high risk*" has not been defined and will be open to interpretation.
- Processing that is likely to result in a *"high risk"* includes, but is not limited to:
  - Systematic and extensive evaluation of individuals (including profiling);

  - » Large scale processing of sensitive data or data relating to criminal convictions; or
  - » Systematic monitoring of a publicly accessible area on a large scale (Article 35(3)).
- The controller is responsible for ensuring that the DPIA is carried out, but must seek advice of the DPO, where designated (Article 35 (2)).
- The processor should also assist the controller in carrying the DPIA (Article 28 (3)(f)).
- The supervisory authority is obliged to make a public list of the type of processing activities which are, and which are not, subject to the requirement for a DPIA, and must communicate those lists to the European Data Protection Advisory Board (**EDPB**) (which will replace the WP29) (Article 35(4) & (5)).
- The GDPR sets out the minimum information which a DPIA should contain, including:
  - » A description of the proposed processing activities; their purpose, and the legitimate interests pursued by the controller;
  - » An assessment of the necessity and proportionality of the processing activities in relation to the purpose;
  - » An assessment of the risks to the rights of data subjects; and
  - » An assessment of the risks, safeguards and security measures proposed to be taken to protect personal data and to demonstrate compliance with the GDPR (Article 35(7)).
- Recital 90 further outlines a number of components of DPIAs.
- Data controllers have flexibility to design and implement the DPIA that is suitable for their processing operations. The WP29 Guidance on DPIAs proposes criteria which controllers can use to assess whether or not a DPIA is sufficiently comprehensive (Annex 2).
- Where appropriate, as part of the DPIA, the controller should seek the views of data subjects or their representatives on the intended processing (Article 35(9)).
- The DPIA should be reviewed, at a minimum, when there is a change of the risk in the processing operations (Article 35(11)).
- Prior consultation with the supervisory authority is required where a DPIA indicates that the processing would result in a *"high risk"* to individuals' rights and the controller cannot find sufficient measures to reduce those risks to an acceptable level. (Article 36(1)).

Business Impact

- The GDPR aims to establish a new culture of privacy by design and by default, by requiring data privacy to be embedded into a business. The privacy by design and by default approach will help businesses to comply with their obligations under the GDPR, as it will ensure that privacy and data protection are considered in the initial stages of a project, and also throughout its lifecycle.
- DPIAs will similarly ensure privacy and data protection issues are addressed at the outset. They will, however, present an extra administrative burden for businesses, both in regard to time and costs. There may also be a difficulty in deciding whether a DPIA is necessary or appropriate given the lack of a definition of "*high risk*" activities. However, it is hoped that the national supervisory authorities will clarify this issue.

Action Points

- Going forward, businesses will have to consider their data privacy obligations when designing and developing new products and services, and throughout their life-cycle.
- Businesses will need to assess whether their data processing activities are likely to result in *"high risk"* to individuals, and if so, ensure that a DPIA is carried out and addresses the specific factors listed in the GDPR. Businesses should consider preparing a template DPIA which can be completed each time it embarks upon a new data processing project.

10 Data Protection Officers (DPOs)

At a glance

- DPOs must be appointed if you are a public body; your primary activities involve large-scale processing of sensitive data or data relating to criminal convictions, or systematic monitoring of data subjects.
- A DPO can be an employee or a contractor, but should have expert knowledge of data protection law.

WHERE TO FIND THIS
Article 37-39, Recital 97
WP29 Guidance on the DPOs

Changes

- The GDPR introduces a mandatory obligation for controllers and processors to appoint a DPO in specified circumstances, including:
  - If you are a public body; or
  - If your core activities require regular and systematic monitoring of data subjects on a large scale; or
  - If your core activities involve large scale processing of sensitive data and data relating to criminal convictions (Article 37(1)).
- The recitals highlight that in the private sector, the *"core activities"* of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities (Recital 97).
- The GDPR does not define what constitutes *"large-scale"* processing, but the WP29 Guidance on DPOs recommends that following factors are considered:
  - the number of data subjects;
  - the volume of personal data;
  - the duration of processing; and
  - the geographical extent.
- Examples of a *"large-scale"* processing include processing of customer data by a bank or by an insurance company.
- The notion of *"regular and systemic monitoring"* is not defined, but examples include: data-driven marketing activities; profiling and scoring for risk-assessment purposes; location tracking; behavioural advertising; and CCTV (WP29 Guidance on DPOs).
- Member States retain a discretion to require the appointment of DPOs in other circumstances (Article 37(4)).
- Group companies can appoint a single DPO, provided that the DPO *"is easily accessible from each establishment"* (Article 37(2)).
- DPOs do not need to be legally qualified. A DPO can be either an employee of the organisation or a contractor, but should have *"expert knowledge of data protection law"*.
- A DPO should not hold a position that leads him or her to determine the purposes and means of data processing. Conflicting positions may include senior management positions, such as CEO or COO, head of marketing or HR (Article 37(5) & (6)).
- If a company does not wish a DPO that has been appointed on a voluntary basis to be subject to the statutory duties of a DPO, it should be made clear in communications with the company that the title of the individual or consultant is not a DPO.
- The GDPR sets out the minimum tasks of a DPO:
  - Inform and advise their colleagues of their data protection obligations;
  - Monitor compliance with the GDPR and the organisation's data protection policies;
  - Provide advice regarding PIAs;
  - Co-operate with the relevant supervisory authority, and
  - Act as a contact point for the supervisory authority on data processing issues (Article 39(1)).

- Organisations are required to provide DPOs with the necessary resources to complete their tasks and for their ongoing training (Article 38(2)). The DPO must not receive any instructions regarding the exercise of his/her tasks; nor be dismissed or penalised for the exercise of those tasks, and must report directly to the highest level of management (Article 38(3)).
- Controllers and processor must publish the contact details of DPOs (where applicable) and communicate these details to the supervisory authority.

Business Impact

- Under the GDPR, all public authorities will have to appoint a DPO. Private sector companies will only have to appoint a DPO: where their primary processing activities involve large-scale systematic monitoring of data subjects (e.g. companies carrying out online behavioural tracking or profiling activities as their core business); or involve large scale processing of sensitive data or data relating to criminal convictions (e.g. cloud companies, who store medical records or other sensitive data, as their core business).
- The WP29 Guidance highlights that DPOs are not personally responsible for non-compliance with the GDPR. It is the controller or processor who is responsible for ensuring that processing is performed in accordance with the GDPR.

Action Points

- Companies should consider now whether they will need to appoint a DPO, and if so, plan how best to recruit, train and resource the position.

11 Data Breach Reporting & Security

At a glance

- Controllers will have a mandatory obligation to report data breaches to their lead supervisory authority within 72 hours, unless the breach is unlikely to result in a "*risk*" to the rights of data subjects.
- A controller may also wish to proactively report the incident to a supervisory authority which is not its lead authority, if it is aware that individuals in other Member States are affected by the breach (WP29 Guidance).
- Controllers will have to notify data subjects where the breach is likely to result in a *"high risk"* to affected data subjects.
- Processors are only obliged to report data breaches to controllers.
- Controllers must keep an internal record of all data breaches.

WHERE TO FIND THIS
Article 32-34, Recital 76, 85-88
WP29 Guidance on Breach Notification

Changes

Notifying Supervisory Authority

- The GDPR introduces a new mandatory obligation requiring controllers **to notify data breaches to the relevant supervisory authority** *"without undue delay, and where feasible, not later than **72 hours** after having become aware of it".* If notification is not made after 72 hours, a reasoned justification for the delay must be provided. However, it is not necessary to notify the supervisory authority where *"the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons"* (Article 33(1)).
- The GDPR defines a *"personal data breach"* as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"* (Article 4(12)).
- The current law contains no legal obligation (other than in the telecommunications sector) to notify the relevant supervisory authority or affected data subjects of personal data breaches. The Irish Data Protection Commissioner (**DPC**) has, however, issued a non-binding code of practice, providing that data breaches should be notified to the DPC's Office.
- The GDPR prescribes the content of the data breach notification to the supervisory authority (Article 33(3)) and to data subjects (Article 34(2)). The breach notification must include:
  a. the nature of the breach, and where possible, the categories and approximate number of data subjects and records concerned;
  b. the contact details of the DPO or other relevant contact;
  c. the likely consequences of the breach; and
  d. the measures taken to address the breach and to mitigate its adverse effects.
- The controller must also keep a record of any data breaches, including its effects and the remedial action taken. This will enable the supervisory authority to verify the controller's compliance with its breach notification obligations (Article 33(5)).
- Where a breach affects data subjects in more than one Member State, and notification is required, the controller should report the breach to its lead authority (Articles 33(1); 56 (1) and 56 (6)).
- A controller may also wish to proactively report the incident to a supervisory authority which is not its lead authority, if it is aware that individuals in other Member States are affected by the breach (WP29 Guidance on Breach Notification).

Notifying Data Subjects

- Controllers must also **notify data breaches to data subjects** where the breach is likely to result in a *"high risk"* to the data subject (Article 34(1)).
- The GDPR does not define what constitutes a *"high risk"* but does provide that notification to data subjects *"will not be required"* where:
  - The controller has implemented appropriate technical and organisational measures that render the personal data unintelligible to anyone not authorised to access it, such as encryption; or

- » The controller has taken subsequent measures which ensure that the high risk to data subjects is not likely to materialise; or
- » It would involve disproportionate effort to contact the data subjects, in which case there should be a public communication instead (Article 34(3)).

- The main objective of notifying data subjects is to provide specific information about steps they should take to protect themselves (Recital 86).
- A processor is obliged to inform the controller of a data breach without undue delay, but has no other notification obligation (Article 33(2)).

Security Obligations

- The GDPR contains enhanced security measures.
- Controllers and processors are required to implement *"appropriate technical and organisational measures"* to ensure a level of security appropriate to the risks that are presented by the processing.
- In particular the controller or processor should consider the risks presented by accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed) (Article 32(1) & (2)).
- *"Appropriate technical and organisational measures"* are described as including (Article 32(1)(a)-(d)):
  - » Pseudonymisation and encryption of data;
  - » The ability to ensure ongoing 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, accessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- The GDPR distinguishes "*anonymous*" data, (namely, data rendered anonymous in such a manner that the individual is not identifiable), from *"pseudonymisation"*, which is data from which the identity of an individual is removed but it can be recovered (e.g. from a numerical identifier) (Recital 26 and Article 4(5) respectively).
- Adherence to an approved code of conduct or an approved certification mechanism may be used to demonstrate compliance with the security obligations.
- Controllers and processors are obliged to take steps to ensure that any individuals acting under their authority, who have access to data, do not process it except on instructions from the controller, unless he/she is required to do so by EU or Member State law (Article 32(4)).

Business Impact

- It is anticipated that the mandatory requirement to report data breaches to supervisory authorities, and in some cases to data subjects, will contribute to an increase in data breach administration and potentially an increase in litigation for non-compliance. The requirement to notify within 72 hours brings with it a significant burden on companies in these circumstances.

Action Points

- Companies should carry out a review of their security measures to ensure they are robust enough to meet the requirements of the GDPR. Data should be rendered unintelligible in case of unauthorised access where possible. As the GDPR approves the use of pseudonymisation as a valid security measure (Article 32(1)(a)), and as a process in implementing data protection by design (Article 25(1)), it would be prudent for companies to consider applying pseudonymisation as a security measure, where personal data cannot be anonymised.
- It is vital for companies to review and revise their data breach response plan to ensure they can manage, contain and respond to breaches quickly, and notify the relevant supervisory authority within 72 hours. To avoid confusion, the response plan should set out the key personnel responsible for dealing with the breach and informing the supervisory authority.
- When drafting a breach response plan, a controller should consider which supervisory authority is the lead authority that it will need to notify.
- Data processing agreements should be reviewed to ensure they include a requirement for the processor to immediately inform the controller of any data breaches.

12 International Data Transfers

At a glance

- Data transfers to countries outside the EEA continue to be prohibited unless that country ensures an adequate level of protection.
- The GDPR retains existing transfer mechanisms, and provides for additional mechanisms, including approved codes of conduct and certification schemes.
- International data transfers are likely to continue to be a challenging issue for multinational companies.
- The GDPR prohibits any non-EEA court, tribunal or regulator from ordering the disclosure of personal data unless it requests such disclosure under an international agreement, such as a mutual legal assistance treaty.

Changes

- The GDPR largely leaves the position regarding international transfers of data unchanged. Like the Directive, the GDPR prohibits the transfer of data to a third country (i.e. a country outside the EEA) unless that country ensures an adequate level of protection (Article 44).
- **Adequacy Decisions** – The Commission retains the ability to decide that a third country or a specified sector within that country or international organisation ensures an adequate level of protection. Transfers of data to such countries will not require specific authorisation (e.g. data transferred from the EEA to 'While-listed' countries or to the US via the Privacy Shield) (Article 45).
- **Appropriate Safeguards** – The GDPR, like the Directive permits transfers to third countries where *"appropriate safeguards"* are in place, such as BCRs or Model Clauses. The GDPR includes two additional mechanisms which suffice as *"appropriate safeguards"*, including: reliance on an approved code of conduct or on an approved certification mechanism, provided that the controller or processor in the third country commits to comply with the safeguards in the code or certification (Article 46).
- **Derogations** – In addition, the GDPR, like the Directive, permits transfers to third countries in specified situations, including where: the data subject has explicitly consented to the transfer; the transfer is necessary for the performance of a contract; for public interest reasons; the defence of legal claims; or the vital interests of the data subject. The requirement for *"explicit"* consent to the transfer is new (Article 49). Where none of the other safeguards or derogations apply, the GDPR permits a transfer to a third country if: it is necessary for the compelling legitimate interests of the controller; is not repetitive; concerns only a limited number of data subjects; and the controller has provided suitable safeguards. The controller must inform the supervisory authority of the transfer (Article 49(1)(g)), Recital 113).
- **Transfers or disclosures not authorised by EU law** – There is a specific provision providing 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, in force between the requesting third country and the EU or Member State (Article 48).

WHERE TO FIND THIS
Articles 44-49, Recitals 108-116

Business Impact

- The GDPR retains the existing transfer mechanisms, but provides additional mechanisms, in particular, approved codes of conduct and certification schemes.

Action Points

- Companies should review their data flows and ensure that they have appropriate international data transfer mechanisms in place such as the Privacy Shield or Model Contracts. International transfers is an area to watch, as it is in a state of flux at the moment.

13 'One Stop Shop'

At a glance

- The GDPR introduces a "lite" one stop shop mechanism.
- Controllers and processors will 'predominantly' be regulated by the supervisory authority where they have their *"main establishment"*, but other *"concerned"* authorities may also be involved in handling complaints about them.

Changes

- The GDPR aims to make it easier for multinational companies to do business across the EU by making them subject to one supervisory authority rather than a supervisory authority in each Member State in which it operates. The GDPR, as adopted, contains a "lite" one stop shop mechanism built on detailed cooperation and consistency provisions (Chapter VII).

Lead Supervisory Authority

- Controllers and processors engaged in cross border processing will be regulated primarily by the supervisory authority in the Member State where they have their *"main establishment" or "single establishment"*. That authority will be the *"lead supervisory authority"* (Article 56(1)).
- *"Main establishment"* is defined as:
  - For controllers, the place of its central administration in the EU will be their main establishment, unless decisions on the processing of personal data are taken in another establishment in the EU which has the power to implement such decisions, in which case that decision-making establishment will be the main establishment.
  - For processors, the place of its central administration in the EU will be their main establishment. If there is none, the establishment where the main processing activities take place will be the main establishment (Article 4(16)).
- Where the criterion of central administration does not apply, the controller should consider where decisions about the means and purposes of processing are given final sign off and where the Director(s) with overall management responsibility for the cross-border processing is located.
- If a controller claims to have its main establishment in one Member State, but no effective and real exercise of management activity or decision-making takes place there, then the lead authority or concerned authorities can rebut the controller's claim. The relevant supervisory authorities will then decide which of them will take the lead in investigations or, in case of conflicting views, the EDPB will decide (WP29 Guidance; Art 65 (1) (b)).

Complaints

- Individuals have the right to lodge complaints with their local supervisory authority. That authority may then, in specified circumstances, handle the complaint. However, the lead authority must be informed of the complaint and may decide to handle the complaint itself. If it does so, the other concerned

WHERE TO FIND THIS
Articles 4, 56, Chapter VII,
Recitals 36, 124-128
WP29 Guidance on Lead
Supervisory Authority

supervisory authority may submit a draft decision which the lead authority will be required to take *"utmost account of"* (Article 56 (3) & (4)).

Cooperation & Consistency

- Lead supervisory authorities and *"concerned"* supervisory authorities in other Member States are obliged to cooperate and endeavour to reach a consensus, and to exchange all relevant information with each other on cross-border issues (Article 60(1)).
- A *"concerned"* supervisory authority is defined as one which is concerned by the processing of personal data because: (a) the controller or processor is established in 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 (Article 4(22)).
- Lead supervisory authorities are further required to provide *"concerned"* supervisory authorities with draft decisions for their opinion, and must *"take due account of their views"* (Article 60(3)).
- Where the lead authority and concerned supervisory authorities cannot reach a consensus, the EDPB will issue a binding decision on the matter (Article 65(1)(a)).
- If a company does not have an establishment in the EU, the mere presence of a representative will not trigger the one-stop-shop system.

Business Impact

- It remains to be seen how effective the "lite" one stop shop mechanism will be in alleviating the need for multinational companies to deal with multiple supervisory authorities. It will also be interesting to see how smoothly the cooperation and consistency mechanisms work in practice.

Action Points

- Companies should ensure they can identify the lead supervisory authority which they will be regulated by, which can be determined according to where their central administration is. This may prove difficult where decisions about different processing activities are taken in different Member States. In the event of uncertainty regarding the lead supervisory authority, companies should map out where the most significant decisions about data processing are made to help determine their *"main establishment"*. Companies should also identify which other supervisory authorities may be *"concerned"* with their activities.

14 Investigative, Corrective & Advisory Powers of Supervisory Authorities

At a glance

- The GDPR includes a long list of specific investigative, corrective, authorisation and advisory powers conferred on supervisory authorities.

WHERE TO FIND THIS
Article 58 & 59

Changes

- The GDPR includes a long list of specific statutory investigative, corrective, authorisation and advisory powers.
- **Investigative powers of supervisory authorities** include (Article 58(1)):
  - Ordering the controller or processor to provide any information required for the performance of its tasks;
  - Carrying out data protection audits;
  - Carrying out a review of certifications which have been issued (all businesses can voluntarily apply for certifications to demonstrate their compliance with the requirements of the GDPR and give data subjects confidence that their data will be protected);
  - Notifying the controller or processor of an alleged infringement of the GDPR;
  - Obtaining access, from the controller or processor, to personal data and information necessary to perform its tasks; and
  - Obtaining access to any premises of the controller or processor.
- **Corrective powers of supervisory authorities**, are similar to those under the Directive, and include (Article 58(2)):
  - Issuing warnings to the controller or processor that intended processing operations are likely to infringe the GDPR;
  - Issuing reprimands to the controller or processor where processing operations have infringed the GDPR;
  - Ordering the controller or processor to comply with the data subject's request to exercise his/her rights;
  - Ordering the controller or processor to bring processing activities into compliance in a specified manner and time frame;
  - Ordering the controller to communicate a personal data breach to the data subject;
  - Imposing a temporary or definitive limitation including a ban on processing;
  - Ordering rectification or erasure of personal data or restriction of processing and notification of such actions to recipients to whom personal data have been disclosed;
  - Ordering the withdrawal of a certification if its requirements are no longer met;
  - Imposing an administrative fine, in addition to or instead of these corrective measures; and
  - Ordering the suspension of data flows to a recipient in a third country or to an international organisation.
- **Authorisation and advisory powers of supervisory authorities** include (Article 58(3)):
  - Advising the controller in accordance with the prior consultation procedure (Article 36);
  - Issuing opinions to the Member State government on any issue related to the protection of personal data;

- » Authorising processing by a controller carried out in the public interest, including in relation to social protection and public health, if Member State law requires such prior authorisation;
- » Issuing opinions and approving draft codes of practice, drawn up by associations and other bodies representing categories of controllers or processors, to ensure the proper application of the GDPR;
- » Accrediting certification bodies;
- » Issuing certifications and approve criteria of certification;
- » Adopting standard contractual clauses for data processing or sub-processing contracts; or for data transfers to non EEA countries (the latter must be approved by the Commission);
- » Authorising contractual clauses between a controller or processor and a controller, processor or recipient of personal data in a non-EEA country or international organisation;
- » Authorising provisions to be inserted into administrative arrangements between public bodies for international data transfers; and
- » Approving binding corporate rules.

- The DPC may bring infringements of the GDPR to the attention of the courts and commence legal proceedings in order to enforce the provisions of the GDPR (Article 58(5)). Member States may, by law, provide for its supervisory authority to have additional powers provided that it does not impair the operation of the cooperation and consistency mechanisms of the GDPR (Article 58(1) & (6)).
- Each supervisory authority must produce annual reports of its activities, including a list of types of infringements notified and types of corrective measures taken, which shall be made available to the public (Article 59).

Business Impact

- The GDPR gives supervisory authorities an extensive list of specific investigative, corrective, advisory and enforcement powers. The DPC's current broad investigative and enforcement powers in relation to civil matters will continue under the GDPR.

Action Points

- Companies should familiarise themselves with the DPC's powers and be ready to cooperate when necessary.

15 Administrative fines

At a glance

- The GDPR provides supervisory authorities with the power to impose significant fines on controllers and processors for non-compliance. Businesses will face fines of up to €20m or 4% of the total worldwide annual turnover of the preceding financial year.
- Fines can be imposed in addition to, or instead of, any corrective measures (such as warnings or reprimands).
- Supervisory authorities will have a degree of discretion as to whether to impose a fine, and the level of that fine. This may lead to divergence throughout the EU in regard to the level of fines imposed.
- Member States may determine whether and to what extent public authorities should be subject to administrative fines.

WHERE TO FIND THIS
Article 83 & 84,
Recitals 148-150
WP29 Guidance on Administritive Fines

Changes

- The DPC currently has broad investigation and enforcement powers but does not have the power to impose fines for breaches of the Data Protection Acts 1988 and 2003. Only the courts may do so in regard to offences committed under the Acts.
- Under the GDPR, supervisory authorities will have wide-ranging powers to enforce compliance, including the power to impose administrative fines (Article 83). Fines can be imposed by a supervisory authority in addition to, or instead of, any corrective measure. A reprimand should only replace a fine in the case of a minor infringement (Recital 148 & Article 83(2)).

Level of Fines

- Fines must be *"effective, proportionate and dissuasive"* (Article 83(1)). There are two maximum thresholds for fines depending on which data protection obligation has been breached.
- Where fines are imposed on an undertaking, an *"undertaking"* should be interpreted in accordance with Articles 101 and 102 of the TFEU (Recital 150). The WP29 further clarifies that under EU case law, an *"undertaking"* should be understood as encompassing an economic unit which may be formed by the parent company and all involved subsidiaries.
- Where fines are imposed on persons that are not an *"undertaking"*, the supervisory authority will take into account the general level of income in the Member State, as well as the economic situation of the person, in considering the appropriate amount of the fine.
- Administrative fines up to **€10m or in the case of an undertaking up to 2% of the total worldwide annual turnover** of the preceding financial year (whichever is greater) shall be imposed for infringement of any one of the following obligations (Article 83(4)):
  - Conditions for obtaining a child's consent (Article 8);
  - Processing which does not require identification (Article 11);
  - Data protection by design and by default obligations (Article 25);
  - Joint controller arrangements (Article 26);
  - Designating a representative in the State where the controller is not established in the EU (Article 27);
  - Obligations of processors (Article 28);
  - Instructions of a controller or processor (Article 29);
  - Records of processing (Article 30);
  - Cooperation with the supervisory authority (Article 31);
  - Security measures (Article 32);
  - Notification of a personal data breach to the supervisory authority (Article 33);
  - Communication of a personal data breach to the data subject (Article 34);
  - Conducting PIAs & Prior consultation (Articles 35 & 36);

- » Designation, position & tasks of the DPO (Article 37-39);
- » Monitoring of approved codes of conduct (Article 41(4)); and
- » Certification mechanisms (Articles 42 & 43).

- Administrative fines **up to €20m or in the case of an undertaking up to 4% of the total worldwide annual turnover** of the preceding financial year (whichever is greater) shall be imposed in respect of a breach of any one of the following obligations (Article 83(5)):
  - » The core data protection principles (Article 5);
  - » The non-personal processing conditions (Article 6);
  - » The conditions for consent (Article 7);
  - » The sensitive personal data processing conditions (Article 9);
  - » Data subjects' rights (including information, access, rectification, erasure, restriction of processing, data portability, objection, profiling) (Articles 12-22);
  - » Transfers of data to third countries (Articles 44-49);
  - » Failure to provide access to premises of a controller or processor (Article 58(1));
  - » Compliance with a specific order or limitation on processing by the supervisory authority or the suspension of data flows (Article 58(2)); and
  - » Obligations adopted under Member State law in regard to specific processing situations (Chapter IX).
- Breaches which fall within the €10m or 2% of annual worldwide turnover category may end up qualifying for the higher tier €20m or 4% of annual worldwide turnover category in certain circumstances.

Assessment Criteria

- The DPC **will have a degree of discretion in relation to the imposition of fines**. When determining whether to impose a fine, and the level of that fine, the DPC may take into account all relevant circumstances including (Article 83(2) (a-k)):
  - » The nature, gravity and duration of the infringement (taking account of the nature, scope and purpose of the processing, number of data subjects affected and level of damage suffered);
  - » The intentional or negligent character of the infringement;
  - » Mitigation measures taken;
  - » The technical and organisational measures implemented;
  - » Any relevant previous infringements;
  - » The degree of cooperation with the supervisory authority to remedy the infringement and mitigate its adverse effects;
  - » Categories of data affected by the infringement;
  - » The manner in which the supervisory authority became aware of the infringement;
  - » Any warnings, reprimands already given by the DPC with regard to the same subject-matter and compliance with those measures;
  - » Adherence to approved codes of conduct; and
  - » Any other relevant aggravating or mitigating factors.
- Recital 148 opens up the possibility to replace a fine by a reprimand, in regard to minor infringements, where the controller is a natural person.

Administrative Fines & Cross-Border Processing

- The EDPB will issue a binding decision on disputes between the lead and concerned authorities relating to the determination of the existence of an infringement (Article 65(1)).
- Lead or concerned authorities may challenge the EDPB's decision by way of an annulment action taken to the EU Court of Justice. An annulment challenge may also be taken by a controller, a processor or a complainant if an EDPB decision is of *"direct and individual concern"* to them (Recital 143).
- The decision of the EDPB may also discuss how the principles of effectiveness, proportionality and deterrence are observed in the administrative fine proposed by the lead supervisory authority. However, any fines imposed will be at the discretion of the lead supervisory authority (rather than the EDPB), and subject to appeal before the national courts where the supervisory authority is established (Article 78 & 83(1)).
- Supervisory Authorities' discretion in relation to the imposition of administrative fines may lead to divergence throughout the EU in relation to the level of fines imposed.
- The WP29 has recommended the creation of a sub-group attached to the EDPB to ensure administrative fines are applied consistently across the EU.

- Member States have discretion in regard to whether and to what extent **public authorities** should be subject to administrative fines (Article 83(7)).

Criminal Sanctions

- The GDPR does not list any criminal offences, rather it defers the task of laying down rules on other penalties to each Member State, who must ensure such penalties are *"effective, proportionate and dissuasive"*. The provisions adopted must be notified to the European Commission by 25 May 2018 (Article 84).

Business Impact

- Unlike in many other Member States, the DPC does not currently have the power to impose administrative fines for infringements of the data protection law. The DPC's power to issue fines under the GDPR (and particularly fines at the limits specified in the GDPR) will significantly increase the risk profile of data protection compliance/non-compliance. If data protection compliance is not currently a boardroom issue, it is certainly likely to be elevated to one in light of the potential consequences of non-compliance.

Action Points

- Companies should be aware of their obligations under the GDPR and should prepare for compliance with the GDPR now in order to mitigate the risk of incurring large-scale fines for non-compliance.

16 Right to Compensation & Liability

At a glance

- Data subjects can sue both controllers and processors for compensation for pecuniary or non-pecuniary damage suffered as a result of a breach of the GDPR.
- Where non-compliance with the GDPR is established, a controller or processor will bear the burden of proving they are not responsible for the event giving rise to the damage.

Changes

- The GDPR seeks to provide data subjects with an ability to recover *"full and effective compensation"* for damage suffered as a result of a breach of the GDPR. The concept of damages is to be interpreted broadly (Recital 146).
- Data subjects will have a right to recover material or non-material damages (Article 82(1)). The recitals include a long list of examples of damage which may arise including loss of control over personal data or limitation of rights, discrimination, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy and *"other significant economic or social disadvantage"* (Recitals 75 and 85).

WHERE TO FIND THIS
Article 82,
Recitals 75 & 146

- The data controller will be responsible for the damage caused by processing which infringes the GDPR. The processor will only be liable insofar as it has failed to comply with its specific obligations under the GDPR or has acted outside of its instructions (Article 82(2)).
- When non-compliance with the GDPR is established, a controller or processor will have to prove that they are not *"in any way"* responsible for the event giving rise to the damage in order to avoid liability (Article 82(3)).
- Where both a controller and processor are engaged in the same processing, and both are responsible for the damage caused, they will be jointly liable for the entire damage (Article 82(4)).
- A controller or processor will be entitled to recover from the other controller or processor that part of compensation paid to a data subject which corresponds to their responsibility for the damage (Article 82(5)).

Business Impact

- The GDPR provides data subjects with a right to recover non-pecuniary loss (such as damages for distress). This is a significant change from the current position under the Data Protection Acts 1988 and 2003. In *Collins v FBD Insurance plc* [2013] IEHC 137, the Irish High Court held that non-pecuniary damage is not recoverable in an action for breach of the duty of care under the Acts.
- With the introduction of joint and several liability between parties engaged in the same data processing, data subjects may choose who to pursue, and are likely to opt for the controller or processor with the biggest pockets. It will then be for the controller and processor to claim back from the other controller or processor, that part of the compensation corresponding to their responsibility for the damage.

Action Points

- Companies should start to prepare for May 2018 in order to mitigate the risk of damages claims from data subjects.
- Liability provisions in contracts, which involve the processing of personal data, will need to be carefully reviewed in light of the recast risk profiles of controllers and processors under the GDPR.

NOTES

KEY CONTACTS

For further information please contact:

John Whelan
Partner
+353 1 649 2234
jwhelan@algoodbody.com

John Cahir
Partner
+353 1 649 2943
jcahir@algoodbody.com

Claire Morrissey
Partner
+353 1 649 2246
cmorrissey@algoodbody.com

Mark Rasdale
Partner
+353 1 649 2300
mrasdale@algoodbody.com

Davinia Brennan
Associate
+353 1 649 2114
dbrennan@algoodbody.com

www.algoodbody.com