Overview of EU General Data Protection Regulation

by Robbie Downing, Baker & McKenzie

Practice note: overview | **Maintained** | European Union

An overview of the nature and scope of data protection and privacy laws in the European Union covering the EU perspective only.

Scope of this note

Significant advancements in the field of information and communication technology and the growth in network interoperability (such as the internet, globally distributed corporate networks and the cloud) have radically increased the ease with which data may be collected, transmitted, stored, manipulated and, most importantly, disseminated.

These developments, together with a general increase in awareness of fundamental rights, particularly the right to privacy, have led to legislative changes and the emergence of a new regime of privacy protection. The number of jurisdictions with data protection or privacy legislation in place has increased significantly during the last decade and the list continues to grow.

This note considers the EU data protection regime set out in the *General Regulation of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (GDPR) from an EU perspective only. It examines the nature and scope of the regime and the rights of data subjects. It also provides information on the obligations of data controllers and data processors and summarises the restrictions on the transfer of personal data outside the EU.

For further information on the current data protection landscape under *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (Data Protection Directive), see *Practice note, Overview of EU data protection regime*.

Nature and scope of the EU data protection regime

The GDPR was adopted in May 2016 and will be directly applicable in all EU member states without the need for transposition on 25 May 2018.

In addition, it is likely that the GDPR will apply in the three members of the *European Economic Area* (EEA) that are not members of the EU through incorporation into Article 7 of and Annex XI to the EEA Agreement.

History and background

The GDPR will replace the Data Protection Directive when it becomes applicable in 2018. The reform was intended to respond to new technological challenges and to put in place a harmonised framework for the protection of personal data. It was felt that the need for national implementation of the Data Protection Directive had led to different

approaches in the member states with regard to the interpretation and enforcement of the basic principles. The choice of an EU regulation as a directly applicable instrument reflects this concern.

The new regime was intended to include activities in the area of police and judicial co-operation. This was covered by the "third pillar" before the Lisbon Treaty came into force in December 2009. As a result, the GDPR is supplemented by *Directive (EU) 2016/680 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data* (*OJ 2016 L 119/89*) (Directive for the police and criminal justice sector). This will replace Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters.

Article 6(2) of the GDPR grants member states a limited right to maintain or introduce more specific provisions to adapt the application of the GDPR with regard to data processing for:

- Compliance with a legal obligation (*Article 6(1)(c)*).
- The performance of a task carried out in the public interest or in the exercise of official authority (*Article 6(1)(e)*).

In particular, member states can determine more precisely specific requirements for data processing including for specified processing situations with a public interest component (*Chapter IX, GDPR*).

This could mean that member states can still enact different procedural and, possibly, substantive requirements to govern certain data processing situations. This gives them the flexibility to take account of domestic legal frameworks as well as cultural sensitivities. However it is likely to reduce the GDPR's harmonising effect. For data controllers that are active in more than one member state, this also means that attention to specific national data protection requirements remains important.

The GDPR attempts to deal with the differences by introducing the consistency mechanism. Supervisory authorities must consult with one another on cross-border decisions and in some instances refer cases to the European Data Protection Board (EDPB) (see *Practice note, EU General Data Protection Regulation: enforcement, sanctions and remedies*).

Territorial scope

The GDPR will apply directly in all member states. This means that the detailed provisions previously included in Article 4 of the Data Protection Directive regarding the question of which national laws apply to the processing of personal data are no longer necessary.

However, it is important for data controllers situated outside the EU to know the circumstances in which their processing activities might be governed by the strict EU regime. This is particularly relevant to two types of processing.

First, the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the EU regardless of whether the processing takes place in the EU or not (*Article 3(1), GDPR*). This is likely to be extended to the EEA. This provision reflects that, in contrast to the current regime, data processors are now specifically included within the scope of the Regulation (see *Obligations of data controllers and data processors*).

Second, the GDPR applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU where the activities relate to either of the following:

- The offering of goods or services to data subjects in the EU, irrespective of whether a payment of the data subject is required (*Article 3(2)(a)*). Recital 23 suggests that a controller or processor that envisages offering services in more than one member state is likely to be caught by this provision. In an online context, the same recital explains that the mere accessibility in the EU of the controller's, processor's or intermediary's website, an email address or other contact details, or the language generally used in the third country where the controller is established, is insufficient to ascertain that intention.

  However, an online provider that uses a language (with the possibility of ordering in that language) or that prices its goods or services in a currency generally used in one or more member states may make it apparent that the controller envisages offering goods or services to data subjects in the EU. This provision is therefore likely to catch many online services established outside the EU if they are processing data of EU customers in the course of their commercial activities.
- The monitoring of the behaviour of data subjects as far as their behaviour takes place in the EU (*Article 3(2)(b)*). This could apply in cases where online providers and advertising networks place cookies or other tracking devices on the equipment of EU data subjects for the purpose of tracking their online behaviour. Other indicators include the subsequent use of personal data processing techniques like profiling a natural person with the intention of making decisions about him or her, or for analysing or predicting his or her personal preferences, behaviours or attitudes (*recital 24*).

The extensive application of the EU data protection regime to non-EU data controllers was strongly opposed during the legislative process, particularly from the US where many leading online services are established. Although many of those services have operations in the EU and are therefore subject to the EU regime already, the GDPR could make it more difficult for the US parent to avoid direct responsibility for compliance.

Where the GDPR applies to a controller or processor not established in the EU, an EU representative must be appointed (*Article 27(1)*), subject to certain exceptions (*Article 27(2)*). The EU representative must be established in one of the member states where the controller or processor offers goods or services or monitors behaviour (*Article 27(3)*).

For further information, see Articles 3 and 27 and recitals 22 to 25 and 80 of the GDPR.

Material scope

Like the Data Protection Directive, the GDPR applies to the processing of personal data:

- Wholly or partly by automated means.
- Other than by automated means, if the data forms part, or is intended to form part, of a filing system.

(*Article 2(1)*.)

This reflects the fact that, although the concept of data protection is closely related to the advent of information technology systems, the protection of individuals should be technologically neutral and not dependent on the techniques used (*recital 15*). A filing system is defined as "any structured set of personal data which are accessible

according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis" (*Article 4(6)*).

There are a number of areas that are excluded from the material scope of the GDPR, including processing activities:

- That fall outside the scope of EU law.
- By member states when carrying out activities that fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) (national security).
- By a natural person in the course of a purely personal or household activity.
- By competent authorities for the purpose of 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 (these activities will be regulated through the provisions of the Directive for the police and criminal justice sector).

(*Article 2(2)*.)

The GDPR does not apply to the data processing activities of the EU institutions, bodies, offices and agencies. These are governed by *Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*. However, that Regulation must be adapted to the principles and rules of the GDPR (*Article 2(3)*).

Household exception

Processing "by a natural person in the course of a purely personal or household activity" is not required to comply with many of the provisions of the Data Protection Directive (*Article 3(2)*). However the scope of this exception with regard to personal data published on the internet was called into question in *Lindqvist v Aklagarkammaren i Jonkoping (Case C-101/01) [2003] ECR I-12971*. The ECJ held that:

- The act of identifying a natural person on an internet site by name or other personal identifiers constitutes "processing" of personal data within the meaning of the Data Protection Directive.
- That processing is only covered by the household exception with regard to processing activities:
  - that are carried out in the course of private or family life of individuals; and
  - provided that the personal data is not made accessible on the internet to an indefinite number of people.

The decision caused some uncertainties, particularly in the context of social networking sites (SNSs) where users often publish not just information about themselves but also about friends, family and colleagues (see *Practice note, Privacy implications of social-networking sites*).

In its 2009 opinion on social networking, the *EU Article 29 Working Party* (WP29) concluded that, although the use of SNSs will generally come under the household exception under Article 3(2) of the Data Protection Directive, not all activities of an SNS user are necessarily covered by that exception.

Article 2(2)(c) of the GDPR largely mirrors the approach taken in the Data Protection Directive. However, recital 18 now includes a non-exhaustive list of household activities, including correspondence and the holding of addresses, or "social networking and online activity undertaken within the context of such personal or household activity". It

also clarifies that the processing must have no connection to a professional or commercial activity. At the same time, it provides that the exception does not apply to the data processing activities of social networking or other online service providers themselves. This means that those providers' use of personal data uploaded to their services in the course of a personal or household activity remains an instance of data processing that is subject to the rules of the GDPR.

For further information see Articles 2 and 3 and recitals 22 to 25 of the GDPR.

National derogations

Member states can introduce exemptions from the GDPR's obligations set out in Articles 12 to 22 (data subjects rights) and Article 34 (communication of a data breach to a data subject), as well as Article 5 (data protection principles) insofar as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- National security.
- Defence.
- Public security.
- Prevention, investigation, detection of criminal offences or the execution of criminal penalties.
- Other important public interests of the EU or member state, in particular economic or financial interests including monetary, budgetary and taxation, public health and social security.
- Protection of judicial independence and proceedings.
- Prevention, investigation, detection and prosecution of breaches of ethics for regulated professions.
- Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests, prevention of crime or breaches of ethics for regulated professions.
- Protection of the individual or the rights and freedoms of others.
- Enforcing matters of civil law.

(*Article 23, GDPR*.)

Chapter IX enables member states to provide exemptions, derogations, conditions or rules in relation to specific processing activities, as follows:

- Freedom of expression and freedom of information.
- Public access to official documents.
- National identification numbers.
- Processing of employee data.
- Processing for archiving purposes and for scientific or historical research and statistical purposes.
- Obligations of secrecy.

- Churches and religious associations.

For further information, see Articles 6(2), 6(3), 9(2)(a), 23 and 85 to 91 and recitals 71, 50, 53 and 153 to 165 of the GDPR.

UK data protection regime after Brexit

The UK Government has confirmed that it will adopt the GDPR in May 2018 (see *Legal update, Government confirms UK will opt into GDPR in May 2018*). It is expected that the UK will adopt a national data protection regime that is largely in line with the EU regime on leaving the EU. This is in order to maintain its status as a third country which provides adequate protection for personal data. This is required under the EU regime to facilitate transfers of personal data outside the EEA (see *Brexit: Watching Brief*).

GDPR: definitions

Data controller and data processor

Most obligations under the GDPR fall on the data controller, who determines the purposes and means of the processing of personal data (*Article 4(7), GDPR*) (tracking the concept with which we are familiar from the Data Protection Directive). The controller can act alone or jointly with others, as under the Data Protection Directive.

In contrast to the Data Protection Directive, the GDPR also imposes specific and separate duties and obligations on data processors. A processor is a "natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller" (*Article 4(8)*).

Personal data and data subjects

The GDPR defines personal data as "any information relating to a data subject" (*Article 4(1)*). A data subject is the identified or identifiable person to whom the personal data relates.

Identifiability

A person is identifiable if he or she "can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity" of that person (*Article 4(1), GDPR*).

To determine whether a person is identifiable, account should be taken of:

- All the means reasonably likely to be used to identify the natural person, including singling out. The concept of "singling out" has been controversial with businesses as it could potentially bring processing activities within the material scope of the GDPR that do not allow the controller to properly identify an individual (for example, by name or address). This could significantly affect online behavioural advertising techniques.

- All objective factors, including the cost of identification, and the amount of time required to identify an individual, taking into consideration the available technology at the time of the processing and technological developments.

(*Recital 26.*)

Pseudonymisation

Drawing from German data protection law, the GDPR creates a new class of personal data, namely data that has undergone pseudonymisation. Article 4(5) defines pseudonymisation as "the processing of personal data in such a manner that it can no longer be attributed to a specific data subject". To maintain personal data in its pseudonymised state, any additional information that identifies the individual must be kept separate from the pseudonymised data.

Recital 26 makes it clear that personal data that has undergone pseudonymisation but which could be attributed to a natural person by additional information should be considered personal data. The GDPR acknowledges that the application of pseudonymisation to personal data can reduce the risk to the data subject and help controllers and processors to meet their data protection obligations. However recital 28 emphasises that the introduction of the new concept is not intended to preclude any other data protection measures. Overall, the GDPR regards pseudonymsation as a data security measure allowing data controllers and processors to show compliance with their obligation under Articles 5(1)(f) and 32.

For more information see *Practice note, Anonymization/Pseudonymization under the GDPR*

Types of personal data

Personal data includes:

- Personal details.
- Family and lifestyle details.
- Education and training.
- Medical details.
- Employment details.
- Financial details.
- Contractual details (for example, goods and services provided to a data subject).

In June 2007, in an opinion that predates the GDPR, the WP29 developed a concept of personal data, which comprises:

- The "common understanding of the concept of personal data" in the EU member states.
- The situations in which national data protection legislation should be applied.
- How it should be applied.

(For more information, see *Legal update, EC Working Party issues opinion on concept of personal data* and *Article 29 Working Party: Opinion 4/2007 on the concept of personal data*.)

The opinion analyses the main elements which make up the concept of personal data and adopts a wide interpretation, particularly on the question of when the information relates to an individual. The WP29 concludes that to establish this, one of three elements should be present:

- **Content.** The information is given about a particular person, regardless of any purpose on the part of the data controller or a third party, or the impact of that information on the data subject (for example, the results of a medical analysis which relate to the patient, and the information contained in a radio frequency identification (RFID) tag, which relate to the holder of the identity document).
- **Purpose.** The data is used, or is likely to be used, to evaluate, treat in a certain way or influence the status or behaviour of an individual. For example, a call log of a telephone call made inside a company office can be used to provide information about the maker and the recipient of the call (for instance, to check what time cleaning staff leave their workplace if they are supposed to confirm by phone at what time they lock the premises).
- **Result.** The use of the data is likely to have an impact on a person's rights and interests (for example, information generated by a satellite location system and then used by a taxi company, which is intended primarily to improve waiting times and fuel efficiency but which also permits the company to monitor the performance of taxi drivers, whether they respect the speed limits, take the most appropriate routes and so on).

The opinion makes it clear that information may relate to an individual even if it does not focus on him or her.

Genetic, biometric and health data

Articles 4(13) and (14) of the GDPR include new definitions of genetic and biometric data.

Genetic data is defined as data "relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that person and which result, in particular, from an analysis of a biological sample from the person in question" (*Article 4(13)*).

Biometric data is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that person, such as facial images, or dactyloscopic data" (*Article 4(14)*).

In addition, Article 4(15) newly defines "data concerning health" as "personal data related to the physical or mental health of a natural person". This includes patient data (that is, information about the provision of health care services, which reveal information about the data subject's health status). This makes it clear that e-health initiatives (such as the UK "Care Data" scheme) that are designed to combine patient data for the purpose of making it available to public and private entities for health care and research purposes must comply with the EU data protection regime.

Online identifiers

Under the Data Protection Directive, there was some debate over whether online identifiers constituted personal data. This issue was partly addressed by the ECJ specifically with regard to IP addresses in its rulings in:

- *Scarlet Extended SA v Societe Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM) (Case C-70/10) [2011] ECR I-11959*, where the court found that IP addresses "are protected personal data because they allow [internet] users to be precisely identified" (see *Legal update, ECJ finds order requiring ISP to filter and block infringing files incompatible with EU law*).
- *Breyer v Bundesrepublik Deutschland (Case C-582/14) [2017] 1 WLR 1569*, where the ECJ ruled that dynamic IP addresses held by a website operator are personal data where the operator has "the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person" (see *Legal update, ECJ rules dynamic IP addresses are personal data*).

However, the GDPR further addresses this question by specifically including online identifiers in the definition of "personal data" in Article 4(1). Recital 30 expands on this by listing a wider range of online identifiers, including IP addresses, cookie identifiers and other identifiers like RFID tags. The recital makes it clear that those identifiers may include any of the traces left by an individual when operating online, which may be emitted or picked up by their devices, applications, tools and protocols and which online service providers can use to create profiles of individuals and identify them.

This potentially widens the definition of "personal data" and could bring most data collected and processed in the context of online behavioural advertising within the scope of the GDPR.

Processing of data

The GDPR applies to the processing of data (*Article 1(1), GDPR*). This is very broadly defined as carrying out "any operation or set of operations" on the data, including:

- Collection.
- Recording.
- Organisation.
- Structuring.
- Storage.
- Adaptation or alteration.
- Retrieval.
- Consultation.
- Use.
- Disclosure by transmission.
- Dissemination or otherwise making available.
- Alignment or combination.

- Restriction (that is, the marking of stored data with the aim of limiting its processing in the future (*Article 4(3)*)).
- Erasure.
- Destruction.

(*Article 4(2)*.)

In effect, any activity involving personal data falls within the scope of the GDPR.

For further information, see Articles 2, 4, 9 and 10 and recitals 1, 2, 26 and 51 of the GDPR.

Data protection principles

The GDPR sets out a number of principles with which data controllers and processors must comply when processing personal data (*Article 5*). These principles form the core of the obligations of the data controller and will usually form the basis of any claim that a data controller has not complied with its statutory duties.

Article 5 includes the following data protection principles:

- **Lawfulness, fairness and transparency.** Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (*Article 5(1)(a)*). The specific requirements for lawful processing are set out in Article 6 (see *Transparency* and *Lawfulness of processing*).
- **Purpose limitation.** Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. (*Article 5(1)(b)*.) (See *Purpose limitation*.)
- **Data minimisation.** Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (*Article 5(1)(c)*). This represents a tightening of the principle contained in Article 6(1)(c) of the Data Protection Directive that the data must not be "excessive". The introduction of a "necessity" requirement is likely to make it more difficult for data controllers to collect data for some general or as yet unspecified future use. The principle may therefore be relevant in the context of big data applications.
- **Accuracy.** Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay (*Article 5(1)(d)*).
- **Storage limitation.** Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (*Article 5(1)(e)*). Personal data may be stored for longer periods provided it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This is subject to the implementation of appropriate data security measures designed to safeguard the rights and freedoms of data subjects.
- **Integrity and confidentiality.** Personal data must be processed in a manner that ensures its appropriate security (*Article 5(1)(f)*). This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. In this regard, data controllers and processors must use appropriate technical or organisational security measures.
- **Accountability.** The data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles (*Article 5(2)*).

For further information, see Article 5 and recital 39 of the GDPR.

Transparency

Specific transparency requirements include the data subjects' right to receive information:

- On the identity of the data controller and the nature of the processing (*Articles 13 and 14, GDPR*).
- About whether or not their personal data is being processed and if so the nature and purposes of that processing (*Article 15*) (see *Rights of data subject*).
- About any personal data breach when that breach is likely to result in a high risk to their rights and freedoms (*Article 34(1)*) (see *Data security*).

Fair and lawful processing information

Certain information must be provided to ensure that the transparency requirement is met with regard to the fair and lawful processing principle. The information that must be supplied depends on whether the data controller collects the data directly from the data subject or obtains the data from a third party.

Data collected from the data subject

If the personal data is collected directly from the data subject, the data controller must provide the data subject with the following information:

- The identity and contact details of the data controller and its representative, if any.
- The contact details of the data protection officer, where applicable.
- The intended purposes of, and the legal basis for, the processing.
- Where the processing is based on Article 6(1)(f) (legitimate interest), the legitimate interest pursued by the data controller or by a third party.
- The recipients or categories of recipients of personal data, if any.
- Where applicable, the fact that the controller intends to transfer the personal data to a recipient in a country outside the EEA or an international organisation, and the existence or absence of a Commission adequacy decision or information about the appropriate or suitable safeguards adduced to secure the data and the means to obtain a copy of them or where they have been made available.

(*Article 13(1), GDPR*.)

The information must be provided at the time the personal data is collected.

At the same time the controller must also provide the data subject with the following information to ensure fair and transparent processing:

- The period for which the data is stored, or the criteria used to determine that period.
- The existence of the data subject's:
  - right of access (*Article 15*);
  - right to rectification (*Article 16*);
  - right to erasure (*Article 17*);
  - restriction of processing (*Article 18*);
  - right to object to processing (*Article 21*); and
  - right to data portability (*Article 20*).
- Where processing is based on the data subject's consent, the right to withdraw that consent at any time.
- The right to lodge a complaint with the supervisory authority.
- Whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract. The data subject must be informed about any obligation to provide personal data and of the consequences of a failure to do so.
- The existence of automated decision-making or profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(*Article 13(2).*)

Data obtained from third parties

If the personal data is obtained from a third party, the controller must provide data subjects with the same information within a reasonable period after obtaining the personal data up to a maximum of one month, having regard to the circumstances in which the data is processed, unless providing the information would involve disproportionate effort (*Article 14(3) and (5)(b)*).

If the personal data is used to communicate with the data subject, then the information must be provided at the time the first communication is sent.

If the data controller intends to disclose the data to a third party, then the information must be provided, at the latest, when the data is first disclosed.

Regardless of whether the data is obtained from the data subject or a third party, the information must be related to data subjects in a concise, transparent, intelligent and easily accessible form, using clear and plain language, particularly if it is addressed specifically to a child (*Article 12(1), GDPR*).

The information must be provided in writing, or by other means, including electronic means, unless the data subject specifically requests provision orally. The burden of proof that the information has been provided falls on the data controller.

For further information, see Articles 12(1), 12(5), 12(7), 13 and 14 and recitals 58 to 62 of the GDPR.

According to the WP29's Action Plan 2017, it will be working on guidelines on transparency in 2017 (see *Legal update, Article 29 Working Party adopts GDPR Action Plan 2017*).

Lawfulness of processing

The GDPR continues the approach under the previous regime requiring a data controller to justify the processing of personal data before it will be considered lawful under Article 5(1)(a) of the GDPR.

Personal data

A data controller must only process personal data on the basis of one or more of the following legal grounds set out in Article 6 of the GDPR:

- The data subject has given his consent to the processing of his data for one or more specific purposes (*Article 6(1)(a), GDPR*) (see *Consent requirements*).
- It is necessary for entering or performing a contract with the data subject (*Article 6(1)(b)*).
- It is necessary for compliance with a legal obligation to which the data controller is subject (*Article 6(1)(c)*).
- It is necessary to protect the vital interests of the data subject (*Article 6(1)(d)*). Recital 46 explains that this legal ground should in principle only be used if the processing cannot manifestly be based on one of the other grounds. It also highlights that some types of processing may serve both important grounds of public interest and the data subject's vital interest (for example, monitoring for epidemics, and their spread, or the processing of personal data in humanitarian emergencies like natural or man made disasters).
- It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed (*Article 6(1)(e)*).
- It is necessary for the purposes of legitimate interests pursued by the data controller or by a third party, except where these interests are overridden by the interests or the fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child (*Article 6(1)(f)*). Public authorities that process personal data in the performance of their tasks may not rely on this condition. When determining whether the data subject's interests or fundamental rights and freedoms override the data controller's legitimate interest, the data subject's reasonable expectations based on the relationship with the controller must be taken into account (*recital 47, GDPR*). The interests and fundamental rights of the data subject could, in particular, override the interest of the data controller where personal data is processed in circumstances where data subjects do not reasonably expect further processing.
- At the same time, processing of personal data that is strictly necessary for the purposes of preventing fraud and for direct marketing purposes is deemed to constitute a legitimate interest of the data controller concerned (*recital 47*). However, in relation to direct marketing, the legitimate interests condition does not override the requirements of the *Privacy and Electronic Communications Directive (2002/58/EC)* (E-Privacy Directive). This requires data subjects' prior consent for electronic direct marketing (for example, by email, text or automated calls). The European Commission has been consulting on the E-Privacy Directive (see *Legal update, European Commission consults on E-Privacy Directive*). The regulators published their responses stating that it should be made clear that the legitimate interests condition does not override prior consent in the E-Privacy Directive. For more information, see Legal updates:
  - *ICO publishes response to European Commission consultation on E-Privacy Directive*;

- *Article 29 Working Party publishes Opinion on review of E-Privacy Directive*; and
- *EDPS publishes Opinion on review of the E-Privacy Directive*.

The European Commission has published a first draft of the proposed new legislation, which takes the form of a Regulation. The Commission is aiming to complete the legislative process by 25 May 2018, to coincide with the GDPR (see *Legal update, European Commission publishes draft E-Privacy Regulation*). The WP29 has published a detailed opinion on the draft E-Privacy Regulation. While generally welcoming the draft, it finds room for improvement in the form of "grave" concerns relating to undermining protections under the GDPR (see *Legal update, Article 29 Working Party publishes opinion on draft E-Privacy Regulation*).

Conditions for laws on which processing can be based
The legal grounds included in Article 6(1)(c) and (e) must be established in accordance with EU or national law (*Article 6(3), GDPR*).

In particular, those laws must determine the purpose of the processing they permit or mandate. To this end, the laws may contain the following "specific provisions" to adapt the application of the GDPR:

- General conditions governing the lawfulness of data processing by the controller.
- The type of data which is subject to the processing.
- The data subjects concerned.
- The entities to which, and the purposes for which, the data may be disclosed.
- The purpose limitation.
- Storage periods.
- Processing operations and processing procedures. This would include measures to ensure lawful and fair processing, including for other specific processing situations as provided for in Chapter IX (see *National derogations*).

Under the previous regime the ECJ clarified that the list of conditions for processing is enumerative and that, in particular, member states were not permitted to adopt laws that impose additional conditions for processing on data controllers (*Asociacion Nacional de Establecimientos Financieros de Credito (ASNEF) v Administracion del Estado (Cases C-468/10 and 469/10) [2011] ECR I-12181*; see *Legal update, ECJ rules that member states must not make processing of personal data subject to additional conditions*). However, Article 6(2) of the GDPR grants member states the right to maintain or adapt more specific provisions with regard to processing for compliance with Article 6(1)(c) and (e). Any such measure must meet an objective of public interest as set out in Chapter IX of the GDPR (*Article 6(2)*) (see *National derogations*).

Sensitive personal data
Subject to certain exceptions, the GDPR prohibits the processing of personal data that reveals:

- Racial or ethnic origin.
- Political opinions.
- Religious and philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data for the purpose of uniquely identifying a natural person.
- Sex life and sexual orientation.

(*Article 9(1).*)

Processing of these types of data is only permitted if the following conditions apply:

- The data subject has given explicit consent to the processing for one or more specific purposes, except where EU or member state law provides that the data subject may not consent to this particular type of processing (*Article 9(2)(a)*).
- It is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, insofar as it is authorised by EU or member state law or a collective agreement pursuant to member state law providing for adequate safeguards for the fundamental rights and the interests of the data subject (*Article 9(2)(b)*).
- Processing is necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent (*Article 9(2)(c)*).
- Processing is carried out:
    - by a not-for-profit entity with a political, philosophical, religious or trade union aim in the course of its legitimate activities;
    - with appropriate safeguards; and
    - solely with regard to members or former members of that entity to persons who have regular contact with it in connection with its purposes.

    Personal data must not be disclosed to anyone outside that entity without the data subject's consent. (*Article 9(2)(d).*)
- Processing relates to personal data which is manifestly made public by the data subject (*Article 9(2)(e)*).
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity (*Article 9(2)(f)*).
- Processing is permitted where it is necessary for reasons of **substantial** public interest, on the basis of EU or member state law which must:
    - be proportionate to the aim pursued;

- respect the essence of the right to data protection; and
- provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

(*Article 9(2)(g)*.)

- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. It must be carried out on the basis of EU or member state law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Article 9(3). (*Article 9(2)(h)*.)
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices. It must be carried out on the basis of EU or member state law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. (*Article 9(2)(i)*.)
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Processing must be based on EU or member state law, which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the data subjects' fundamental rights and interests. (*Article 9(2)(j)*.)

Member states have the right to maintain or introduce further conditions, including limitations, with regard to genetic, biometric or health data (*Article 9(4)*).

Criminal convictions and offences are not classified as sensitive personal data. Instead, the GDPR provides additional safeguards in connection with the processing of personal data "relating to criminal convictions and offences or related security measures based on Article 6(1) which shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects." (*Article 10, GDPR*.)

For further information, see Articles 6 to 10 and recitals 38, 40 to 50 and 59 of the GDPR.

Consent requirements

The GDPR defines consent as a "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 his or her personal data (*Article 4(11)*).

Form of consent

A statement can include a written statement (including by electronic means) or an oral statement.

Examples of affirmative actions include:

- Ticking a box when visiting a website.

- Choosing technical settings for an online service.
- Any other conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data.

(*Recital 32, GDPR*.)

Silence, pre-ticked boxes or inactivity should not normally constitute consent. When the processing has multiple purposes, consent should be given for all of them (*recital 32*).

The data controller must be able to demonstrate that "the data subject has consented to processing of his or her personal data." (*Article 7(1)*.) For consent to be informed, the data subject should be aware of at least the data controller's identity and the intended purposes of the processing (*recital 42*).

If consent is given in the context of a written document that also concerns other matters (such as a contract), data controllers must present the requirement to give consent to the processing of personal data in a way that is distinguishable from these other matters (*Article 7(2)*). This provision is likely to cause issues for online providers, which will have to ensure that the way in which they obtain user consent allows them to comply with their legal obligations while, at the same time, not interrupting or otherwise affecting the user's online experience.

Organisations should review their contracts, terms and conditions and other documents to ensure that the section on consent is clearly identifiable and clearly written.

Withdrawal of consent

Data subjects have a right to withdraw their consent at any time, although this will not affect the lawfulness of any processing carried out before the withdrawal (*Article 7(3), GDPR*). Data subjects must be informed of their right to withdraw their consent and consent must be as easy to withdraw as to give. This is likely to affect the practice where the granting of consent is made easy for users, for example by ticking a box on a website, but the withdrawal of consent requires an email or even a postal notification.

Freely given consent

When determining whether consent is in fact "freely given" utmost account must be taken of whether the performance of a contract or the provision of a service is conditional on the consent to the processing or use of data that is not necessary for the execution of the contract (*Article 7(4), GDPR*). Recital 43 also explains that, to ensure that consent is freely given, it should not provide a legal ground for data processing where there is a clear imbalance between the data subject and the data controller. The recital specifically states that consent is unlikely to be freely given where the data controller is a public authority. In keeping with previous practice, it probably also continues to be unlikely that consent can be freely given by employees to their employers' data processing activities (see *Practice note, EU General Data Protection Regulation: implications for employers*).

For further information see *Practice note, Employee consent under the GDPR.*

Implied consent

It is not yet clear if there is any scope for implied consent to be valid, but the WP29 may address this point in its guidance on consent, which it is working on in 2017.

For further information on consent, see Articles 4(11), 6(1)(a), 7, 8 and 9(2)(a) and recitals 32, 38, 40, 42, 43, 51, 59 and 171 of the GDPR.

Children's consent

Questions may arise as to the reliability of consents obtained from children, particularly in an online environment, given that they may not yet be capable of fully understanding the nature of the processing to which they are agreeing.

There are relatively few specific provisions arising from the processing of children's personal data. The GDPR stipulates the following in relation to the offering of online services:

- Personal data of children below the age of 16 can only be processed on the basis of consent "if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child."
- Member states have the right to lower the age threshold for the parental consent to the age of 13 but not lower.
- The data controller must make reasonable efforts to verify parental consent taking into consideration available technology.

(*Article 8.*)

For further information, see Article 8 and recitals 38, 58 and 71 of the GDPR.

According to the WP29 Action Plan 2017, it will be working on guidelines on consent in 2017 (see *Legal update, Article 29 Working Party adopts GDPR Action Plan 2017*).

Purpose limitation

As a general rule, the purpose limitation principle binds the data controller to the specified, explicit and legitimate purposes notified to the data subject on collection of the personal data (*Article 5(1)(b), GDPR*). Further processing of the data beyond that which was originally anticipated is only permitted as long as the new processing activity is not incompatible with that original purpose.

Exceptions to the purpose limitation principle

However, the GDPR includes three notable exceptions to this rule.

Further processing with the data subject's consent

Further processing of personal data for a purpose incompatible with that for which the data was originally collected is permitted if the data subject consents to this new processing activity (*Article 6(4), GDPR*). This is likely to mean that the controller must notify the data subject of its intention to use the data for the new purpose (*recital 50*) and that it must not process the data for that new purpose until it has obtained the data subject's consent.

Further processing on the basis of an EU or member state law

Personal data can be processed for further incompatible purposes on the basis of an EU or member state law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) (*Article 6(4), GDPR*) (see *National derogations*).

If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, EU or member state law may determine and specify the tasks and purposes for which the further processing shall be regarded as compatible and lawful (*recital 50*).

In theory, this would, for example, permit member states to adopt laws that would authorise the subsequent use (including the disclosure to public authorities and further processing by those authorities) of personal data initially collected by private entities for their own commercial purpose. This is a significant departure from the current legal restrictions and would potentially allow public authorities much more leeway to access existing data pools on the basis of laws which might be adopted after those data pools came into existence.

Further processing for public interest purposes

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will not be considered to be incompatible with the original purposes. This type of further processing of existing data is therefore generally permitted, subject to certain conditions.

Further compatible processing

In all other cases, when ascertaining whether a purpose of further processing is compatible with the one for which the data was originally collected, data controllers must take into account the following non-exhaustive list of criteria:

- Any link between the purposes for which the personal data has been collected and the purposes of the intended further processing.
- The context in which the personal data has been collected, in particular regarding the relationship between the data subjects and the controller.
- The nature of the personal data, in particular whether sensitive personal data is processed, or whether personal data related to criminal convictions and offences is processed.
- The possible consequences of the intended further processing for data subjects.
- The existence of appropriate safeguards, which may include encryption or pseudonymisation.

(*Article 6(4), GDPR*.)

For further information, see Articles 6 to 10 and recitals 38, 40 to 59 of the GDPR.

Notification and registration requirements

Although the Data Protection Directive provided for a general obligation on data controllers to notify the processing of personal data to the supervisory authorities, this obligation was ultimately seen to produce "administrative and financial burdens" that were disproportionate to the effect the practice had on the protection of personal data (*recital 89, GDPR*). Critics often referred to the notification process as "tick-box compliance" that added little to the actual data protection practices of businesses and individual data controllers.

For this reason, it was decided to abolish "such indiscriminate general notification obligations" and replace them with "effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes." (*Recital 89.*) Examples of such processing operations include those that involve using new technologies, or are of a new kind and where data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing (*recital 89*).

The obligation to notify the supervisory authority is replaced with the data controller's "accountability" obligation to demonstrate compliance with the data protection principles (*Article 5(2)*).

For more information on the data controller's obligations, see *Obligations of data controllers and data processors*.

Rights of data subject

Chapter III of the GDPR includes a number of rights of the data subject. For more information see *Practice note, Data Subject Rights Under the GDPR.*

Data subject access

Data subjects have the right to obtain confirmation from the data controller as to whether or not the data controller processes personal data relating to them (*Article 15, GDPR*).

If the data controller does process the data subject's personal data, it must provide the data subject with access to the data. It must also provide the following information:

- The purposes of the processing.
- The categories of personal data concerned.
- The recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organisations.
- Where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period.
- The right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- The right to lodge a complaint with a supervisory authority.
- Where the personal data is not collected from the data subject, any available information as to its source.

- The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

If the data controller or data processor transfers the personal data to a third country or to an international organisation, they must inform the data subject of the appropriate safeguards in relation to the transfer (*Article 15(2), GDPR*).

The controller must also provide the data subject with a copy of the personal data undergoing processing (*Article 15(3)*). The first copy of the information must be provided free of charge. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.

If the data subject makes the subject access request by electronic means, and unless otherwise requested by the data subject, the controller must provide the information in a commonly used electronic form.

For further information, see Articles 12 to 15 and recital 63 of the GDPR.

Rectification and erasure

Section 3 of Chapter III includes:

- The existing right to rectification (*Article 16*).
- An express right to erasure ("right to be forgotten") (*Article 17*).
- Right to restriction of processing (*Article 18*).
- Right to data portability (*Article 20*).

Right to rectification

Based on the principle set out in Article 5(d), the data subject has the right to request the data controller to:

- Rectify any personal data relating to them that is inaccurate.
- Complete any incomplete data, including by way of supplementing a corrective statement.

This requirement is more specific than the equivalent requirement included in the Data Protection Directive, particularly with regard to incomplete data.

For further information, see Articles 12, 16 and 19 of the GDPR.

Right to erasure ("right to be forgotten")

Data subjects have the general right to obtain from the data controller the erasure of personal data concerning him or her without undue delay. The controller must comply with this request, if one of the following grounds applies:

- The data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.
- The data subject withdraws consent on which the processing is based, and there is no other legal ground for the processing of the data.
- The data subject objects to the processing of personal data pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing (see *Processing for public interest purposes and the controller's legitimate interest*).
- The data subject objects to the processing of their data for direct marketing purposes (including profiling to the extent that it is related to direct marketing).
- The personal data has been unlawfully processed.
- The personal data has to be erased for compliance with a legal obligation under EU or the national law to which the data controller is subject.
- The personal data has been collected in relation to the offer of information society services directly to a child.

(*Article 17(1), GDPR*.)

Article 17(2) includes a new "right to be forgotten". This requires the data controller to erase personal data, if the controller:

- Is required to erase the data under Article 17(1).
- Has made that data public (for example, if the controller has published the information on the internet or where it has shared the data with third parties).

This new right requires the controller to inform other controllers that are processing the personal data that the data subject has requested erasure by them of any links to, or copies of, that data.

The original data controller's obligation only applies to the extent that the steps (including technical measures) it is required to take are "reasonable". It is likely that further guidance will be required to establish the extent of this obligation.

Both the right to erasure under Article 17(1) and the right to be forgotten under Article 17(2) do not apply to the extent that they would collide with certain public policy interests. Data controllers are not required to erase the data or inform third party controllers of the data subject's request to the extent that the processing is necessary for any of the following reasons:

- Exercising the right of freedom of expression and information.
- Compliance with a legal obligation which requires processing by EU or national law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For reasons of public interest in the area of public health in accordance with Article 9(2)(h) and (i) and Article 9(3).
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), insofar as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing.
- For the establishment, exercise or defence of legal claims.

(*Article 17(3), GDPR*.)

For further information, see Articles 17 and 19 and recitals 65 and 66 of the GDPR.

Restriction of processing

Data subjects have the right to obtain from the data controller a restriction of processing in certain circumstances (*Article 18, GDPR*).

This means that the data controller has the continued right to store the data, but may only process it in one of the following circumstances:

- With the data subject's consent.
- For the establishment, exercise or defence of legal claims.
- For the protection of the rights of another natural or legal person.
- For important public interest reasons.

The right to restriction of processing therefore provides a lower level of protection that pragmatically takes into account the potential usefulness of the data to data subjects themselves, the data controller or third parties.

The right to restriction of processing exists where one of the following conditions applies:

- The data subject contests the accuracy of the data. The data subject can request for the data to be restricted for a period enabling the data controller to verify the information.
- The processing is unlawful and the data subject opposes the erasure of the data and chooses their restriction instead. This could be the case where the data subject wishes to secure the data for evidential purposes.
- The controller no longer needs the data for its own purposes but is required to retain it by the data subject for the establishment, exercise or defence of legal claims.
- The data subject has objected to processing pending verification as to whether the legitimate grounds of the controller override those of the data subject (see *Right to object to processing*).

(*Article 18(1)*.)

In cases, where a data subject has obtained a restriction, the data controller must inform him or her before the restriction is lifted (*Article 18(3)*).

For further information, see Articles 18 and 19 and recital 67 of the GDPR.

Obligation to notify data subject

The data controller must also communicate any rectification, erasure or restriction of processing to each recipient to whom it has disclosed the personal data, unless this proves impossible or involves disproportionate effort (*Article*

19, GDPR). The data controller must inform the data subject, on request, about the recipients to whom it has made the data available.

Right to data portability

Article 20(1) of the GDPR introduces a new right to data portability. This means that the data subject has the right to obtain from the data controller, on request, a copy of all personal data, which he or she has provided to the controller, provided the following conditions are met:

- The processing is based on the data subject's consent (*Article 6(1)(a)* and *Article 9(2)*) or on a contract (*Article 6(1)(b)*).
- The processing is carried out by automated means.

The data subject also has the right to transmit the data to another controller without being hindered by the controller to which the data was originally provided. Where technically feasible, the data subject can request to have the data transmitted directly from one controller to another (*Article 20(2)*).

The data controller must provide the data in a structured, electronic format that is commonly used and permits further use by the data subject.

The right to data portability is targeted in particular at online service providers and is designed to promote further interoperability between online systems. Data subjects are to be enabled to move their data seamlessly from one online provider to another without losing any data previously disclosed to an online service or having to re-input such data. The provision is clearly aiming to create a more level playing field between online providers which have established a strong position making it difficult for new entrants to gain a foothold because of the effort required for users to move their accounts.

Article 20(4) restricts the right to data portability to the extent that it "adversely affects the rights and freedoms of others". This provision is closely linked to a claim by online providers, who see the personal data they collect about their customers (and particularly the structured format in which this data is held) as one of their main business assets. An obligation to provide this data for free to their customers and, by implication, their competitors, is therefore seen as threatening a number of business models. However, a restriction proposed by the Council during the legislative process that stated that this right should not apply if disclosing personal data would infringe intellectual property rights in relation to the processing of that data was ultimately rejected. This leaves online providers with the more generic "rights and freedoms" argument to put forward in defending their commercial objectives.

For further information, see Articles 12 and 20 and recital 68 of the GDPR.

WP29 has adopted the final version of its guidelines on data portability, having considered comments on its initial version and related FAQs that were published in December 2016 (see *Legal update, Article 29 Working Party publishes GDPR guidelines on DPIAs for consultation and adopts final guidelines on DPOs, data portability and lead supervisory authority*).

Right to object to processing

Processing for public interest purposes and the controller's legitimate interest

Article 21(1) of the GDPR grants the data subject, on grounds relating to the data subject's particular situation, a "right to object" to processing that is being conducted on the basis of either of the following:

- Article 6(1)(e) (processing necessary for a task carried out in the public interest or in the exercise of official authority vested in the data controller).
- Article 6(1)(f) (processing necessary for the purpose of the legitimate interest of the data controller or a third party).

The right to object is based on Article 14 of the Data Protection Directive, with some modifications regarding the burden of proof. Where this right is exercised, the processing must stop, unless the controller demonstrates compelling legitimate grounds for the processing which override the data subject's rights and freedoms, or where the processing is necessary for the establishment, exercise or defence of legal claims.

This differs from the approach taken under the Data Protection Directive, where the data subject had to establish compelling legitimate grounds that would override the data controller's right to process the data for public interest purposes or for his or her own legitimate interests. The GDPR therefore grants the data subject a prima facie right to stop the processing. The data controller must rebut this in order to continue the processing.

Processing for direct marketing purposes

Data subjects have the right to object, at any time, to the processing of their personal data for direct marketing purposes (including profiling to the extent that it is related to direct marketing) (*Article 21(2), GDPR*). The right must be explicitly offered to the data subject in an intelligible manner and so that it is clearly distinguishable from other information.

Formal requirements

The data controller must explicitly bring the right to object to the data subject's attention at the time of the first communication with the data subject (at the latest) (*Article 21(4), GDPR*). This information must be presented clearly and separately from any other information.

In the context of the use of information society services, data subjects must be able to exercise their right to object by automated means using technical specifications (*Article 21(5)*).

Exception

Where the data is processed for scientific or historical research purposes or statistical purposes, the data subject's right to object is restricted where the processing is necessary for a task carried out in the public interest (*Article 21(6)*).

For further information, see Article 21 and recitals 69 and 70 of the GDPR.

Measures based on profiling

Data subjects have the right not to be subject to a decision evaluating their personal aspects that is based solely on automated processing, including profiling, and produces legal effects concerning or significantly affecting them (*Article 22(1), GDPR*).

A data subject could be subject to an automated decision based on profiling if:

- It is necessary for entering into, or performance of, a contract.
- It is authorised by EU or member state law to which the data controller is subject and that lays down suitable measures to safeguard the data subject's legitimate interest.
- It is based on the data subject's explicit consent.

(*Article 22(2)*.)

Safeguards

In cases where the profiling is carried out for contractual purposes or based on the data subject's consent, the data controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. These measures must include the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. This is designed to prevent situations where important decisions about the availability of services or access to information are made purely on the basis of algorithmic calculations over which the data subject has no control and of whose logic he or she is in most cases not aware (that is, the "computer says no" problem).

Profiling using sensitive personal data

A decision based on profiling must not be based on sensitive personal data unless one of the following conditions applies:

- The data subject has given their explicit consent to that processing (*Article 9(2)(a), GDPR*).
- The processing is necessary for reasons of substantial public interest (*Article 9(2)(g)*).

(*Article 22(4)*.)

In both cases the data controller must take suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

For further information, see Articles 4(4), 9 and 22 and recitals 71 and 72 of the GDPR.

According to the WP29's Action Plan 2017 it will be working on guidelines on profiling in 2017 (see *Legal update, Article 29 Working Party adopts GDPR Action Plan 2017*).

Right to request delisting of search results

In May 2014, the ECJ ruled that EU citizens have the right to request internet search engines to remove search results in response to a query for their name, if those results are outdated or irrelevant. Where the search engine rejects a request, data subjects can complain to the relevant supervisory authority. (*Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD) (Case C-131/12) [2014] QB 1022*; see *Legal update, ECJ confirms right to have search engine results removed where they affect privacy rights*.) In response to the decision, both the WP29 and supervisory authorities (including the UK Information Commissioner) have issued guidance on how national supervisory authorities intend to implement the judgment and the criteria they will use when responding to a claim by data subjects following a search engine's refusal to delist (see *Article 29: Guidelines* and *Information Commissioner: Search result delisting criteria*).

For information on the obligation to remove links from search engine results, see *Checklist, Removal of links from search engine results*.

Obligations of data controllers and data processors

In contrast to the Data Protection Directive, the GDPR imposes a significant burden for demonstrating compliance with the data protection regime not only on the data controller but also on the data processor, which contributes to the overall principle of accountability.

For more information see *Practice note, Demonstrating compliance with the GDPR.*

Appointment of a data processor

The data controller is required to enter into a contract or other legally binding act with the processor that must impose the following obligations on the processor:

- Process the personal data only on the documented instructions of the controller, including with regard to international data transfers to a third country or an international organisation. This is likely to mean that data processors cannot use cloud computing technology or services without the data controller's approval.
- Comply with security obligations equivalent to those imposed on the controller under Article 32 of the GDPR.
- Only employ staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality.
- Enlist a sub-processor only with the prior permission of the controller.
- Assist the controller in carrying out its obligations with regard to requests by data subjects to exercise their rights under Chapter III of the GDPR (including the right to transparency and information, the data subject access right, the right to rectification and erasure, the right to the restriction of processing, the right to data portability and the right to object to processing).
- Assist the data controller in carrying out its data security obligations under Articles 32 to 36 of the GDPR.

(*Article 28(3), GDPR.*)

At the data controller's request, the data processor must also delete or return all personal data to the controller at the end of the service provision (*Article 28(3)(g)*). It must make available to the data controller information that demonstrates the processor's compliance with its obligations and allow for, and contribute to, audits and inspections (*Article 28(3)(h)*).

A processor must not appoint sub-processors without the specific or general written consent of the data controller (*Article 28(2), GDPR*). Where a sub-processor is appointed, the contract between the processor and the sub-processor must reflect the data protection obligations set out in the contract between the controller and the processor (*Article 28(4)*).

Chapter IV of the GDPR includes a number of obligations for data controllers and data processors. For further information see *Practice note, Data processor obligations under the GDPR: Overview*

Appointment of a data protection officer

Data controllers and data processors must designate a data protection officer (DPO) in any of the following circumstances:

- Where the processing is carried out by a public authority or body, except for courts acting in their judicial capacity.
- Where the core activities of the controller or the processor consist of processing operations, which, by virtue of their nature, their scope and their purposes, require regular and systematic monitoring of data subjects on a large scale.
- Where the core activities of the controller or the processor consist of processing sensitive personal data on a large scale and data relating to criminal convictions and offences (*Articles 9 and 10, GDPR*).

(*Article 37(1)*.)

Given the lack of precision in these provisions, some controllers and entities may find it difficult to ascertain whether the requirement applies to them.

Article 37(4) also suggests that member states retain the ability to require the appointment of DPOs in other situations.

The DPO may fulfil the tasks as a staff member of the controller or processor or on the basis of a service contract (*Article 37(6)*). The grounds on which a DPO's position can be terminated are not specified, although Article 38(3) makes it clear that DPOs must not be dismissed or penalised by the controller or the processor for performing their tasks. It remains to be seen whether this will be sufficient to ensure the independence of DPOs in cases of conflict.

Article 38(5) includes a confidentiality obligation on the DPO concerning the performance of his or her task. The controller or processor must ensure that the fulfillment of the DPO's tasks does not result in a conflict of interest (*Article 38(6)*).

For further information, see Articles 37 to 39 and 83 and recital 97 of the GDPR.

The WP29 has adopted the final version of its guidelines on DPOs, having considered comments on its initial version and related FAQs that were published in December 2016 (see *Legal update, Article 29 Working Party*

publishes GDPR guidelines on DPIAs for consultation and adopts final guidelines on DPOs, data portability and lead supervisory authority).

Documentation requirements

Article 30 of the GDPR introduces documentation requirements for both data controllers and data processors.

Obligations of the data controller

The data controller and, where applicable, its representative, must maintain a record of all processing operations under their responsibility (*Article 30(1), GDPR*). This record must include at least the following:

- The name and contact details of the controller, or any joint controller or processor, and of the representative, if any.
- The name and contact details of the DPO, if any.
- The purposes of the processing.
- A description of categories of data subjects and of the categories of personal data relating to them.
- The recipients or categories of recipients of the personal data. This includes the controllers to whom personal data is disclosed, including recipients in third countries or international organisations.
- Where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation. In the case of transfers that include one-off or infrequent processing of limited amounts of personal data in the legitimate interest of the data controller or processor, the appropriate safeguards must also be documented (see *Article 49(1)*).
- Where possible, a general indication of the time limits for erasure of the different categories of data.
- The description of the technical and organisational security mechanisms the data controller employs.

Obligations of the data processor

The data processor and its representative (where applicable) must maintain a record of all categories or processing activities carried out on behalf of a controller (*Article 30(2)*). This includes the following information:

- The name and contact details of the processor or processors and of each controller on behalf of which the controller is acting, and of the controller's representative (if any).
- The name and contact details of the processor's DPO (if any).
- The categories of processing carried out on behalf of each controller.
- Where applicable, the categories of transfers of personal data to a third country or an international organisation.
- Where possible, a general description of the data security measures put in place by the processor.

Exceptions

The documentation requirement does not apply to controllers and processors that employ fewer than 250 persons unless they fulfill at least one of the following conditions:

- The processing they carry out is likely to result in a risk for the rights and freedoms of the data subject.
- The processing is not occasional.
- The processing includes sensitive personal data or data relating to criminal convictions and offences (*Articles 9(1) and 10, GDPR*).

(*Article 30(5)*.)

For further information, see Article 30 and recital 82 of the GDPR.

Risk to data subjects' rights and freedoms

Recital 75 of the GDPR clarifies that risks to the rights and freedoms of data subjects may be of varying likelihood and severity and may result from any of the following:

- Processing that gives rise to:
  - discrimination;
  - identity theft;
  - fraud;
  - financial loss;
  - damage to reputation;
  - loss of confidentiality of personal data protected by professional secrecy;
  - unauthorised reversal of pseydonymisation; or
  - any other significant economic or social disadvantage.
- Processing that reveals sensitive personal data relating to the data subject.
- Processing where personal aspects are evaluated ("profiling"), in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.
- Processing of personal data relating to vulnerable persons, in particular children.
- Processing that involves a large amount of personal data and affects a large number of data subjects ("big data processing").

The likelihood and severity of the risk must be determined by reference to the nature, scope, context and purposes of the processing (*recital 76*). Risk must be evaluated on the basis of an objective assessment. The EDPB is intended to provide further guidance on these questions (*recital 77*).

Data protection impact assessment

Data controllers must conduct an impact assessment (DPIA) before undertaking any processing that presents a specific privacy risk by virtue of its nature, scope or purposes (*Article 35, GDPR*).

Activities for which a DPIA is needed

The GDPR sets out a list of situations in which a DPIA is required. These include the following:

- A systematic and intensive evaluation of personal aspects relating to natural persons based on automated processing on which decisions are based that produce legal effects for that person or significantly affect him or her. This includes profiling.
- Processing sensitive personal data or data relating to criminal convictions or offences on a large scale.
- A systematic monitoring of a publicly accessible area (for example, through CCTV) on a large scale.

(*Article 35(3)*.)

Contents of the DPIA

The DPIA must cover at least the following:

- A systematic description of the envisaged processing operations and the purposes of the processing, including where applicable the legitimate interest pursued by the controller.
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
- An assessment of the risks to the rights and freedoms of data subjects referred to in Article 35(1).
- The measures envisaged to address the "risk, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned".

(*Article 35(7), GDPR*.)

For further information, see Articles 35, 36 and 83 and recitals 84 and 89 to 96 of the GDPR.

The WP29 has adopted an initial version of guidelines on DPIAs and determining whether processing is "likely to result in a high risk" for the purposes of the GDPR. This version is open to public consultation until 23 May 2017, after which a final version will be adopted (see *Legal update, Article 29 Working Party publishes GDPR guidelines on DPIAs for consultation and adopts final guidelines on DPOs, data portability and lead supervisory authority*).

The WP29's draft guidelines aim to promote the development of:

- A common EU list of processing operations for which a DPIA is mandatory. The WP29 has developed specific criteria which can trigger the need to carry out a DPIA. As a rule of thumb, a processing operation which meets

less than two of the criteria may not require a DPIA. However this is not an absolute rule and the circumstances surrounding each processing operation have to considered individually. A DPIA is a continual process and should be reassessed every three years.

- A common EU list of processing operations for which a DPIA is not necessary.
- Common criteria on the methodology for carrying out a DPIA. The draft guidelines include a diagram setting out the generic process for a DPIA.
- Common criteria for establishing when the supervisory authority shall be consulted.
- Recommendations where possible, building on the experience gained in EU member states.

Annex 1 contains a list of links to examples of existing DPIA frameworks (both generic and sector-specific) and to international standards containing DPIA methodologies for reference. Annex 2 sets out the criteria for an acceptable DPIA by reference to the relevant GDPR provisions.

Data protection by design and by default

The data controller is obliged to implement data protection measures "by design and default" when processing personal data (*Article 25(1), GDPR*). This means that the controller must implement appropriate technical and organisational measures, like pseudonymisation, in an effective manner, to ensure compliance with data protection principles.

To this end, data controllers must take into account the following:

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

Data controllers must take measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is processed (data minimisation) (*Article 25(2)*). That obligation applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility. In particular, those measures must protect the data subject from the unauthorised sharing of their data with an indefinite number of third parties by default.

Data controllers may use approved certification mechanisms (in accordance with Article 42 of the GDPR) to demonstrate compliance with this obligation (*Article 25(3)*).

For further information, see Article 25 and recital 78 of the GDPR.

Codes of conduct and certification mechanisms

The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate compliance. Signing up to a code of conduct or certification scheme is not obligatory.

For further information, see Articles 40 to 43 and recitals 98, 99 to 100, 148, 150 and 151 of the GDPR.

According to the WP29 Action Plan 2017, it will be working on guidelines on certification (see *Legal update, Article 29 Working Party adopts GDPR Action Plan 2017*). Guidelines on certification are expected to be "pre-adopted" in June 2017 (see *Legal update, Article 29 Working Party publishes GDPR guidelines on DPIAs for consultation and adopts final guidelines on DPOs, data portability and lead supervisory authority*).

Data security

Data controllers and data processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected (*Article 32(1), GDPR*).

Controllers and processors must ensure that anyone acting under their authority who has access to the personal data does not process it except on their instructions, unless required to do so by EU or member state law (*Article 32(4)*).

Security measures

Measures data controllers and data processors may take include or display the following features and functionalities:

- The pseudonymisation and encryption of personal data.
- The ability to ensure the 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, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(*Article 32(1), GDPR*.)

Assessing risks

Controllers and processors must take account of the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons (*Article 32(1), GDPR*).

When assessing the appropriate level of security, controllers and processors must take account of the risks presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed (*Article 32(2)*).

Data security breach

Articles 33 and 34 establish a mandatory system in relation to the breach of data security. Data controllers must notify any personal data breach to their national supervisory authority and, in certain instances, the data subject.

The new notification requirement largely mirrors the breach notification system established under Article 4(3) of the E-Privacy Directive. This imposes a similar requirement on providers of publicly available electronic communications systems. The E-Privacy Directive is currently under review and the European Commission has published a first draft of its proposed Regulation, which it is aiming to finalise by 25 May 2018 to coincide with the deadline for adoption of the GDPR (see *Legal update, European Commission publishes draft E-Privacy Regulation*). The draft proposes removing separate security obligations for electronic communications providers (which will now be covered by the GDPR), but introduces customer notification of specific security risks.

The WP29 has published a detailed opinion on the draft (see *Legal update, Article 29 Working Party publishes opinion on draft E-Privacy Regulation*).

Notification to supervisory authority

The controller is required to notify breaches to their national supervisory authority without undue delay and in any event within 72 hours of becoming aware of them (*Article 33(1), GDPR*). Processors must inform their controller "without undue delay after becoming aware" of a breach, including prescribed information (*Article 33(2)*).

No notification requirement exists with regard to breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons".

There are detailed formal requirements for the notification to a supervisory authority. The notification must at least:

- Describe the nature of the personal data breach, including the categories and number of data subjects concerned, and the categories and approximate number of data records concerned.
- Communicate the identity and contact details of the DPO or other contact point where more information can be obtained.
- Describe the consequences of the personal data breach.
- Describe the measures proposed or taken by the controller to address the personal data breach.

(*Article 33(3)*.)

The controller must document any personal data breach, including its effects and any remedial action taken (*Article 33(5)*).

Notification of data subjects

If the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the controller must also communicate the personal data breach to them without undue delay (*Article 34(1), GDPR*).

The notice must describe in clear and plain language the nature of the personal data breach and contain at least information about:

- The identity and contact details of the DPO or other contact point where more information can be obtained.
- The consequences of the personal data breach.

- The measures proposed or taken by the controller to address the personal data breach.

(*Article 34(2).*)

There is no need to inform data subjects of the breach if any of the following conditions are met:

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

For further information, see Articles 33, 34, 83 and recitals 85, 87 and 88 of the GDPR.

According to the WP29's Action Plan 2017, it will work on updating existing opinions and referentials on personal data breach notification in 2017 (see *Legal update, Article 29 Working Party adopts GDPR Action Plan 2017*).

Cross-border data transfers

Like the Data Protection Directive, the GDPR restricts transfers of personal data outside the EU in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

Personal data can only be transferred outside the EU to third countries or international organisations in compliance with the conditions for transfer set out in Chapter V (*Articles 44- 50*) of the GDPR.

The prohibition applies to data controllers and data processors and extends to "onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation." (*Article 44.*)

Adequacy decisions

The Commission may make findings of adequacy in relation to a third country, and also in relation to a territory or specific sectors in a third country or an international organisation (*Article 45(1), GDPR*). Transfers made on this basis do not require further authorisation from a national supervisory authority.

Article 45(2) sets out the rules for assessing adequacy which are more prescriptive than under the Data Protection Directive. They include the need to ensure that the third country offers levels of protection that are "essentially equivalent to that ensured within the Union", and provide data subjects with effective and enforceable rights and means of redress.

Adequacy decisions adopted by the Commission on the basis of Article 25(6) of the Data Protection Directive are preserved until amended, repealed or replaced under Article 45 of the GDPR (see *Practice note, Cross-border transfers of personal data: Community findings of adequacy*). The Commission is required to review all decisions

on an ongoing basis from the date the GDPR enters into force and to act if the level of data protection in any country, territory of sector has fallen below the required standard (*Article 45(4), GDPR*).

Adequate safeguards

Transfers of personal data can be made in the absence of adequacy decisions where the data controller or data processor receiving the personal data has provided adequate safeguards, on condition that enforceable data subject rights and effective legal remedies for data subjects are available (*Article 46, GDPR*).

Safeguards may be provided by way of:

- A legally binding and enforceable instrument between public authorities.
- Binding corporate rules (BCRs).
- Standard contractual clauses adopted by the Commission.
- Standard contractual clauses adopted by a supervisory authority and approved by the Commission.
- An approved code of conduct.
- An approved certification mechanism.

Standard contractual clauses

Standard contractual clauses can be adopted by the Commission or adopted by supervisory authorities and approved by the Commission. Transfers on this basis will not require approval by national supervisory authorities. This removes an existing administrative burden in some member states.

Contractual clauses can also be agreed between the parties and authorised by the competent supervisory authority (*Article 46 (3)(a), GDPR*).

Standard contractual clauses could be included in a contract between EU based data processors and processors in a non-EU country (processor to processor model clauses) (*recital 168*).

Commission decisions on standard contractual clauses remain in force until amended, repealed or replaced by the Commission. Ongoing monitoring is not required for these decisions under the GDPR as for adequacy decisions). Current standard contractual clauses are subject to legal challenge (see *Practice note, Cross-border transfers of personal data: Standard contractual clauses*).

Binding corporate rules (BCRs)

There is specific legal recognition for BCRs in Article 47 of the GDPR. BCRs may not only be used within the same corporate group but can also be used by a group of enterprises engaged in a joint economic activity. There is a new single approval mechanism for BCRs under the consistency mechanism at Article 63. BCRs are available for data controllers and data processors established in an EU member state and must confer enforceable rights on data subjects with regard to the processing of their personal data.

BCR approvals given on the basis of Article 26(2) of the Data Protection Directive continue to be applicable, although it may be appropriate to review the approvals held.

According to its workplan, the WP29 will publish guidelines on data transfers based on BCRs and contractual clauses in 2017.

Approved codes of conduct and approved certification mechanisms

Codes of conduct and approved certification mechanisms are new mechanisms to adduce adequacy. Guidelines on certification are expected to be "pre-adopted" in June 2017 (see *Legal update, Article 29 Working Party provides update on GDPR implementation guidance, Privacy Shield and enforcement matters*). In both cases the transfers must be on the basis of binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Derogations

Article 49 of the GDPR sets out a limited number of derogations which can be used for data transfers in the absence of adequacy determinations or appropriate safeguards.

The derogations are similar those in the Data Protection Directive. They include the following:

- The individual has explicitly consented after being informed of the risks of the transfers due to the absence of an adequacy decision and appropriate safeguards.
- Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.
- Necessary for the performance of a contract made in the interests of the individual between the controller and another person.
- Necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent.
- Necessary for important reasons of public interest or to establish, exercise or defend legal claims.
- The transfer is made from a public register which is intended to provide information to the public and specific conditions are fulfilled.
- The transfer is in the controller's legitimate interests. This can only apply if no other derogations are applicable; in respect of occasional transfers concerning only a limited number of data subjects which are necessary for the legitimate interests of the data controller. The data controller is additionally required to provide appropriate safeguards for the personal data and to inform both the supervisory authority and the data subjects of the transfer. The assessment and the safeguard applied must be documented in accordance with Article 30. Its application is likely to be of limited use for many data controllers.

The first three derogations are not available for public authorities in the exercise of public powers.

Privacy Shield

On 6 October 2015 the ECJ issued its decision in *Schrems v Data Protection Commissioner (Case C-362/14) [2016] QB 527* declaring the safe harbour framework invalid (see *Legal update, ECJ rules that the EU-US safe harbor arrangement is invalid*).

On 12 July 2016 the European Commission issued an implementing decision on adequacy of the protection provided by the EU-US Privacy Shield. The Privacy Shield imposes stronger obligations on companies in the US to protect personal data and stronger monitoring and enforcement by the US Department of Commerce and the Federal Trade Commission.

The Privacy Shield will continue to apply under the GDPR and will continue in force as the UK goes through the Brexit process. The first annual review of the Privacy Shield will take place in September 2017 (see *Legal update, MEPs pass non-legislative resolution on the Privacy Shield calling for proper assessment*).

The Privacy Shield contains important changes:

- Written commitments and reassurances from the US Government that access for national security and law enforcement purposes to personal data transferred to the US is subject to clear limitation, safeguards and oversight.
- The creation of an Ombudsperson who will follow up on complaints and enquiries by EU individuals into access to data for national security purposes.
- An annual review and suspension clause, designed to reassure data subjects that US Government commitments will be maintained even if there is a change in the US administration.
- EU supervisory authorities will play a more important role in enforcement.

Consequences of non-compliance
Breach of the GDPR data transfer provisions is identified in the band of non-compliance issues for which the maximum level of fines of up to 4% of global turnover can be imposed.

Businesses that infringe the provisions of the GDPR dealing with international transfers of personal data may be subject to administrative fines up to EUR 20,000,000 or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

For further information, see Articles 44 to 50 and recitals 103 to 114, 117 to 119 and 167 to 169 of the GDPR.

According to the WP29's Action Plan 2017, it will work on updating existing opinions and referentials on data transfers to third countries (see *Legal update, Article 29 Working Party adopts GDPR Action Plan 2017*).

Enforcement, sanctions and remedies

The GDPR provides data subjects and national supervisory authorities with significant powers to enforce its provisions and obtain compensation for its breach. Among other things, supervisory authorities are granted:

- A number of investigative, corrective and authorisation and advisory powers (*Article 58, GDPR*).
- The power to impose administrative fines on controllers and processors (*Article 83*).

Data subjects have a right to lodge a complaint with the competent supervisory authority (*Article 77*). They also have a right to an effective judicial remedy against a supervisory authority and against infringing controllers and processors (*Articles 78 and 79*).

Supervisory authorities are required to co-operate with each other and with the newly created EDPB to ensure the consistent enforcement of the GDPR (*Articles 60-76*).

For detailed information about enforcement, sanctions and remedies under the GDPR, see *Practice note, EU General Data Protection Regulation: enforcement, sanctions and remedies*.

According to the WP29's Action Plan 2017, it will be working on guidelines on administrative fines, the setting up of the EDPB, and the preparation of the one stop shop and the EDPB consistency mechanism (see *Legal update, Article 29 Working Party adopts GDPR Action Plan 2017*).

END OF DOCUMENT

