Baker McKenzie.

Robert Half®

protiviti®
Face the Future with Confidence

Frequently Asked Questions

Understanding the General Data Protection Regulation

Without question, the EU General Data Protection Regulation disrupts security and privacy procedures by mandating that organisations focus on *protecting the individual* as opposed to *controlling organisational processes*.

INTRODUCTION

The General Data Protection Regulation (GDPR) has arrived at last — and with it, a wealth of questions, concerns and challenges for any organisation conducting commerce with citizens in the European Union. We are pleased to offer some answers here.

After four years of negotiations, the European Union's GDPR was adopted on April 14, 2016, and went into effect on May 25, 2018. Organisations subject to the regulation were given a grace period of two years to review current practices and procedures, but they are now required to be in compliance with every GDPR requirement. (See sidebar for timeline of events leading to the GDPR.)

The GDPR has two high-level objectives: Harmonise the previously fragmented legacy legislation among EU Member States, and address public perceptions that doing business on the internet is inherently risky. Many concerns arise from the wide publicity given to successful cybercrime attacks resulting in personal data theft. The explosive use of mobile devices, adoption of big data analytics, and increased volumes of personal data being digitally generated, processed and shared have exposed personal identities to greater risk than at any time in recorded history. Bottom line, the GDPR aims to make the online environment more trustworthy and harmonised.

Without question, the GDPR disrupts security and privacy procedures by mandating that organisations focus on *protecting the individual* as opposed to *controlling organisational processes*. The content of the GDPR is undoubtedly extensive, nuanced and, in many places, open to some interpretation. Organisations have many questions. In response, Baker McKenzie, Robert Half and Protiviti have partnered to develop this resource guide that addresses the many aspects of this new regulation.

Please note that information provided is not intended to be legal analysis or advice, nor does it purport to address every aspect of the GDPR or other data privacy requirements. Companies should seek the advice of legal counsel or other appropriate advisors on specific questions as they relate to their unique circumstances.

Timeline of Events Leading to the GDPR

- October 1995: Data Protection Directive (95/46/EC) is adopted. The majority of the rules of the GDPR are the same as or similar to those of the Data Protection Directive. Thus, much of the GDPR has been with us for more than 20 years.
- January 2012: First draft of the GDPR is released.
- March 2014: European Parliament votes to support the GDPR.
- December 2015: The Trilogue (EU Commission, European Parliament and EU Council of Ministers) reaches an agreement about the GDPR.
- April 2016: European Parliament and the Council of the EU formally adopt the GDPR with a two-year grace period before enforcement.
- May 2018: GDPR enforcement begins on May 25.

TABLE OF CONTENTS

GDPR INSIGHTS

01 What is the EU General Data Protection Regulation?

The EU General Data Protection Regulation (GDPR) is a pan-European data protection law that was passed in May 2016 following years of intense negotiations among the various EU institutions and Member States. It is intended to strengthen individuals' rights in relation to personal data and make data protection fit for the digital age.

The GDPR went into effect May 25, 2018, and was immediately enforced as law in all Member States of the European Union, with the aim of it being incorporated into the European Economic Area (EEA) Agreement in June 2018.

02 What legislation is the GDPR replacing?

The GDPR supersedes the EU Data Protection Directive of 1995, as well as much of Member States' existing national data protection legislation implementing the Directive (under the Directive, each Member State was required to implement the Directive by way of national legislation).

03 Will there be national legislation implementing the GDPR?

As the GDPR is a regulation, no implementing legislation will be required. Rather, the GDPR will be directly applicable across the EU. However, the GDPR contains various so-called opening clauses giving Member States ample room to supplement the GDPR in certain areas (such as data protection in the employment context). Therefore, each Member State is expected to enact national legislation supplementing the GDPR. As of May 2018, only Germany and Austria have such legislation in place.

04 What is the territorial scope of the GDPR? (Article 3)

The GDPR has a very wide territorial scope. It applies to the processing of personal data by data controllers and data processors established in the EU. But importantly, it also applies to data controllers and data processors not established in the EU to the extent their processing activities relate to the offering of goods or services to data subjects within the EU, or to the monitoring of their behaviour. Effectively, any organisation outside the EU is likely to fall under the GDPR to the extent its products or services are targeted at EU individuals.

05 How does the GDPR define personal data? (Article 4)

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

The GDPR has a very wide territorial scope. It applies to the processing of personal data by data controllers and data processors established in the EU. In addition, any organisation outside the EU is likely to fall under the GDPR to the extent its products or services are targeted at EU individuals.

06 Are online identifiers personal data? (Recital 30)

Potential examples of online identifiers are some IP addresses, cookies and RFID tags. In the digital world, data subjects are increasingly associated with online identifiers provided by their devices, applications, tools and protocols. When combined with unique identifiers and other information received by servers, they may be used to create profiles of the data subjects and identify them; in this case, they qualify as personal data under the GDPR.

07 What is considered "sensitive" personal data? (Article 9)

The GDPR refers to sensitive personal data as "special categories of personal data." These include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs (or lack thereof), trade union membership, health, or a natural person's sex life or sexual orientation. These categories are generally the same as those in the Data Protection Directive. Importantly, special categories of personal data under the GDPR also include "genetic data" and "biometric data," so long as such data is processed for the purpose of uniquely identifying a natural person. Sensitive data is subject to stricter protections as the likelihood and severity of risks to the rights and freedoms of individuals stemming from the processing of such data are considered high.

08 Are records of criminal convictions/ sentences considered "special" personal data? (Article 10)

Personal data relating to criminal convictions and offences are not in a "special" category of personal data under the GDPR. However, under the GDPR, the processing of such data is subject to special restrictions similar to those applying to the processing of special categories of data. In addition, the processing of this type of data must be carried out under the control of an official authority unless otherwise authorised by EU or Member State law providing for appropriate safeguards.

09 What is a data subject?

Under the GDPR, a data subject is any natural person who is "in" the European Union. The person does not need to be a citizen or resident of the EU, so even the processing of data relating to persons visiting the EU would fall under the GDPR to the extent that personal data is collected while on EU soil. We await guidance from the relevant authorities on how the words "in the European Union" are to be interpreted.

10 What are the data protection principles? (Article 5)

At the core of the GDPR is a set of principles relating to the processing of personal data. These are not new but the GDPR now expressly requires data controllers to be able

to demonstrate compliance with these principles ("accountability"):

- **Lawfulness, fairness and transparency** — Data is processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation** — Data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data** minimisation — Data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- **Accuracy** — Data which is inaccurate must be erased or rectified without delay.
- **Storage/retention limitation** — 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 personal data is being processed.
- **Integrity and confidentiality** — Data is processed in a manner that ensures appropriate data security.

11 What is data protection by design and by default? (Article 25)

The GDPR codifies the longstanding concepts of data protection by design and by default and translates them into privacy obligations for data controllers.

Data protection by design means that data protection safeguards should be embedded in the design specifications of services, products, systems or processes from the earliest stage of development rather than being addressed as an afterthought. Data controllers are required to take the protection of data into consideration during the full lifecycle of any potentially new service, business process or supporting IT system that may use personal data. Under Article 25, data controllers are required to:

- Implement appropriate technical and organisational measures which are designed to implement data protection principles (such as data minimisation) in an effective manner.
- Integrate necessary safeguards into their processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

These obligations are quite vague and what measures will be appropriate in a particular instance will depend on the state of the art and implementation costs, as well as on the risks resulting from the processing.

Data protection, by default, means that appropriate security/privacy settings must automatically be applied to any data processing. For example, no manual configuration change to settings should be required by the user to make the product/service more secure, but privacy-friendly default settings are in place. Additionally, by default, the personal data must be kept only for the amount of time (i.e., "storage limitation") required to provide the product/service. Organisations should not use pre-ticked consent boxes.

12 When is data processing lawful? (Article 6)

As was the case under the Directive, under the GDPR, data processing is generally prohibited. Data processing is only lawful if and to the extent at least one of the following conditions applies:

- The data subject has given **consent** to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the **performance of a contract** to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for **compliance with a legal obligation** to which the data controller is subject.

- Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person.
- Processing is necessary for the performance of a **task carried out in the public interest** or in the **exercise of official authority** vested in the data controller.
- Processing is necessary for the purposes of **legitimate interests** pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of a data subject which require protection of personal data, in particular where the data subject is a child.

Note that the above applies to ordinary or general personal data; there are more stringent requirements for the processing of **sensitive personal data**.

13 What are the conditions for consent? (Article 7)

The GDPR retains the concept of consent as we know it from the Data Protection Directive, but overall, it will become more difficult to rely on consent as a justification for data processing. Consents obtained under the Directive will continue to be valid if they conform to the GDPR requirements. Under the GDPR, consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or clear affirmative action, signify agreement to the processing of personal data relating to them. In a nutshell:

- For consent to be **unambiguous**, it requires a clear affirmative action by the data subject, meaning that silence, pre-ticked boxes and inactivity will no longer suffice for there to be valid consent. This is probably the most significant change in relation to consent brought in by the GDPR.
- For consent to be **freely given**, the data subject must have a genuine and free choice and must be able to refuse or withdraw consent at any time without detriment. Consent is not freely given if there is a clear imbalance between the data subject and the data controller.
- For consent to be **specific**, it must relate to specific processing operations, meaning that broad consents to unspecified processing operations will likely be invalid. Consent must also cover all purposes for which data processing is carried out, requiring data controllers to determine and specify those purposes in advance.
- For consent to be **informed**, data controllers must give data subjects sufficient information so they understand the fact that and the extent to which they are consenting. Data subjects must also be aware, at a minimum, of the identity of the data controller and the purposes of the relevant processing.

While it is generally sufficient for consents to be given orally, it is highly recommended that consents are obtained in written (including electronic) form, as the onus is on the data controller to establish that consent has been obtained.

Where consent is relied upon to legitimise the processing of sensitive data, profiling activities or cross-border data transfers, it needs to be "explicit." The meaning of "explicit consent" needs to be extracted from interpretations and guidance from supervisory authorities and depends on the context in which consent is obtained.

14 Is parental consent required to process personal data of minors? (Article 8)

Parental consent will be required to process the personal data of children under the age of 16 for online services. Individual Member States may legislate for a lower age of consent, but this may not be below the age of 13.

15 Does the GDPR apply to data processing in an employment context? (Article 88)

Yes, as a general rule, it does. However, the GDPR authorises EU Member States to put in place more specific rules for the processing of employees' personal data in the employment context. Consequently, each Member State may come up with its own rules for the processing of data in the employment context, which multinational employers will need to be aware of. In general, employment law is not harmonised across the EU.

16 What technology requirements does the GDPR dictate be in place?

Although the GDPR prescribes that appropriate technical and organisational measures are put in place to protect the security of personal data, the nature of the measures is left to those whose job it is to put them in place.

17 How will the GDPR be enforced for non-EU companies?

The GDPR has specific requirements regarding the transfer of data out of the EU. One of these requirements is that the transfer must only happen to countries deemed as having adequate data protection laws. In general, the EU does not list the United States as one of the countries that meets this requirement.

For U.S. companies that wish to be able to receive personal data to which the GDPR applies, the EU and the United States have agreed on a system known as Privacy Shield, which will be enforced by the U.S. Federal Trade Commission. Privacy Shield is designed to create a programme whereby participating companies are deemed as having adequate protection, and therefore facilitate the transfer of information. In short, Privacy Shield allows U.S. companies, or EU companies working with U.S. companies, to meet this requirement of the GDPR.

The GDPR retains the concept of consent as we know it from the Data Protection Directive, but overall it will become more difficult to rely on consent as a justification for data processing.

18 What is the European Data Protection Supervisor?

The European Data Protection Supervisor (EDPS) is an independent supervisory authority whose primary objective is to ensure that European institutions and bodies respect the right to privacy and data protection when they process personal data and develop new policies.

19 What is the European Data Protection Board?

The European Data Protection Board (EDPB) replaces the Article 29 Working Party set up under the 1995 Directive. Its primary role is to foster the consistent application of the GDPR across Member States and promote cooperation between national supervisory authorities. It also issues guidelines and recommendations. Article 70 contains a detailed list of the EDPB's specific tasks. The EDPB has legal personality status and is composed of the heads of the national supervisory authorities of the Member States and the head of the EDPS, or their delegates.

20 How does the GDPR align with GAPP?

The Generally Accepted Privacy Principles (GAPP) is a framework of the United States and Canada that facilitates the management of privacy policies and programmes on a local, national and international level. Accountants, among other professionals, face a number of differing privacy legislation and regulations. The GAPP can offer a comprehensive framework for designing an effective privacy programme that can be applied in a number of industries and professions. GAPP will continue to provide useful guidance.

21 Will audits of GDPR compliance be conducted by the EU privacy authorities?

A regulator can proactively come in to an organisation to assess it and make sure it is in line with GDPR requirements, or the regulator can come in based on a breach that the organisation has had to personal data. The regulator will be looking for proof that the organisation's board of directors is aware of the GDPR and the personal data risks. The regulator needs to ensure that the organisation has assessed the scope of GDPR within that organisation. The GDPR is a risk-based regulatory framework and the organisations have the ability to choose the right controls for the risk profile, as long as they can justify those controls to regulators when they come knocking on their door.

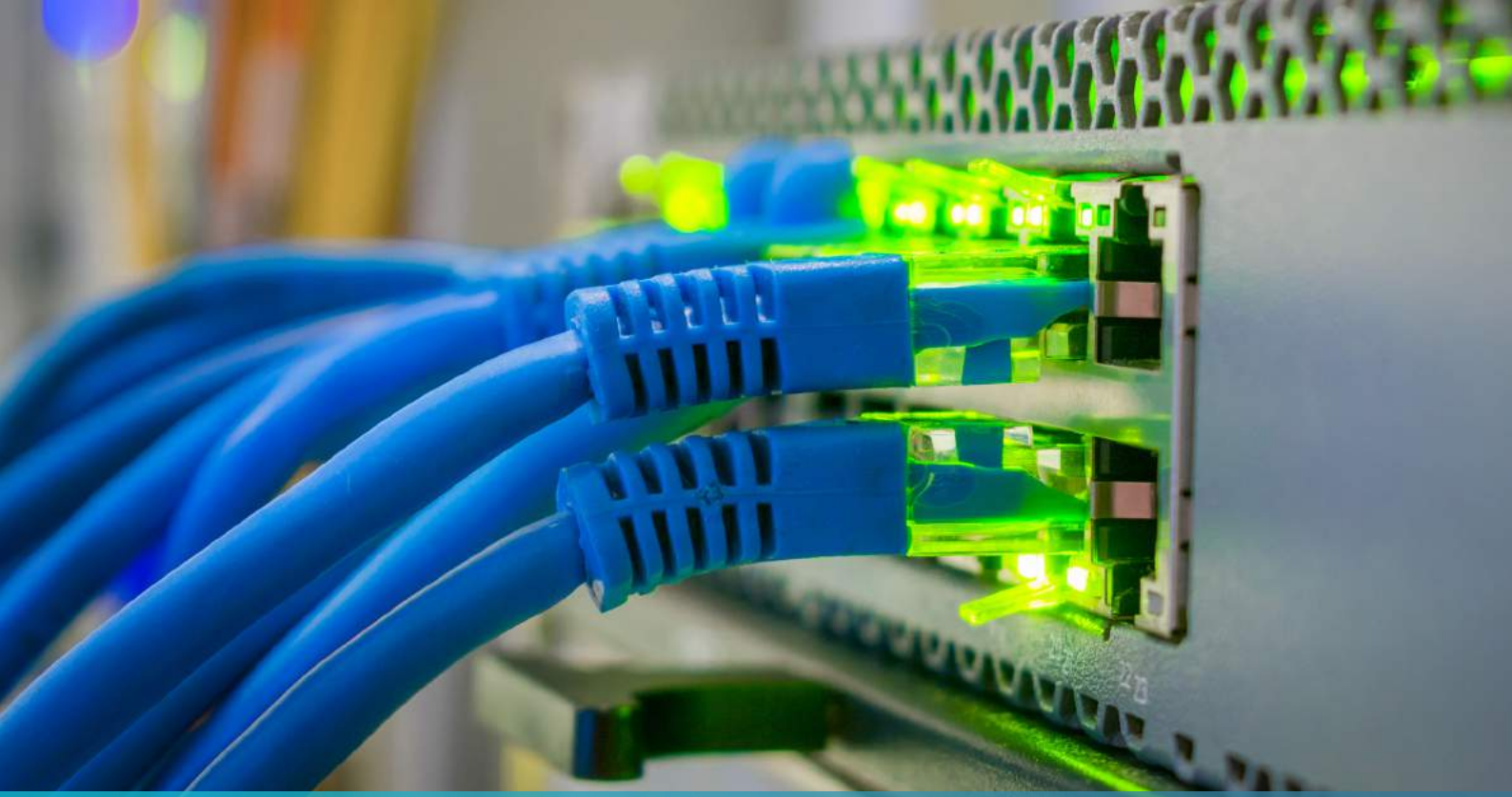
22 What is the cornerstone of the process of becoming GDPR compliant?

The single most important thing about GDPR compliance is disciplined execution. A GDPR compliance strategy is worth very little without disciplined execution. Having the most perfect policies and staff instructions is worth nothing without proper operationalisation of policies and the development of a culture of commitment to data protection.

23 How will compliance with the GDPR affect compliance approaches for other regulations with which organisations must comply?

This is a complicated question. Beyond the GDPR, there are numerous regulations worldwide that contain information security, data privacy, breach notification and documentation provisions with which affected organisations must continue to comply. These include, to name just a few, the Payment Card Industry Data Security Standard (PCI-DSS), the U.S. Sarbanes-Oxley Act, the U.S. Health Insurance Portability and Accountability Act (HIPAA), and for organisations in the financial services industry, the second Payment Services Directive (PSD2), Markets in Financial Instruments Directive (MiFID II), as well as various anti-money laundering regulations in jurisdictions around the world. These regulations variously include requirements on the collection, use and retention of data as well as steps organisations are expected to take in the event of security breaches.

While the intent of GDPR is not to preclude data processing that is necessary for compliance with a legal obligation, there unquestionably are conflicts and differing requirements between the GDPR and these and other regulations. Organisations will want to consult with their legal counsel and other experts to assess their current compliance practices and determine how they can maintain compliance with all of the regulations, including the GDPR, to which they are subject.



RIGHTS OF THE DATA SUBJECT

24 What information must be provided to data subjects? (Articles 12-14)

It must be remembered that the safety and security of a data subject's personal data is a fundamental human right in Europe. Accordingly, one of the key objectives of the GDPR is the fostering of transparency of data processing and strengthening of data subjects' rights. In this spirit, Articles 13 and 14 contain long lists of information that controllers need to give to data subjects. Article 13 applies in situations where data is collected directly from the data subject. Article 14 applies where data has been obtained from another source. Not all of the information items listed are new, but the list is certainly more extensive than it was under the Directive and implementing Member State law. The information to be provided to data subjects by the controller includes:

- Information about the data controller
- Contact details of any data protection officer (if applicable)
- The intended purposes of the processing and the legal basis for such processing
- The recipients or categories of recipients to whom the data is disclosed
- Specific details regarding any intended cross-border transfers
- The data retention period
- Various rights of data subjects (e.g., rights to access, erasure and data portability; right to object to certain processing; right to withdraw consent; and the right to complain to the supervisory authority)
- Whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract
- Whether the data subject is obliged to provide the data and the potential consequences of a failure to provide the data
- The existence of any automated decision-making, the logic involved, and the potential consequences of such processing on the data subject

25 How must information provided to data subjects be communicated? (Article 12)

Information must be provided (free of charge) to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Generally, the information must be provided in writing or electronic form.

Companies must be able to provide a copy of the data subjects' records in electronic format if requested. Where possible, data controllers should also be able to provide remote access via a secure system.

26 What is the individual's right of access? (Article 15)

Article 15 gives individuals the right to obtain confirmation from the data controller as to whether personal data concerning the data subject is being processed, and if so, the right to access the data and the following information:

- The purpose(s) of the processing
- The categories of personal data concerned
- The recipients to whom data will be disclosed, along with any relevant information on cross-border transfers of the data
- The envisaged data retention period or at least the criteria for determining that period
- The existence of the data subject's right to request the correction or erasure of personal data and the right to restrict, or object to, processing
- The right of data subjects to complain to the supervisory authority
- Where the personal data is not collected from the data subject, any available information as to the source
- The existence of automated decision-making, the logic involved, and the potential consequences and significance of such processing on the data subject

Companies must be able to provide a copy of the data subjects' records in electronic format if requested. Where possible, data controllers should also be able to provide remote access via a secure system (Recital 63). If requested by a data subject, the information may be provided orally.

In cases where the data controller has reasonable doubts regarding the identity of a person making an information request, the data controller may request additional information necessary to confirm the identity of the person.

Where rights, and freedoms of others (e.g., IPR, trade secrets or copyright protected software), conflict with data subjects' access rights, then data controllers might have an obligation to refuse certain access rights (Recital 63). In addition, data controllers may be able to narrow the scope of an access request where they process large volumes of data concerning an individual.

27 What is the right to rectification? (Article 16)

Data subjects have the right to obtain from the data controller correction of inaccurate personal data without undue delay. They also have the right to have incomplete personal data completed.

28 What is the right to erasure? (Article 17)

Article 17 provides individuals with a right to request the deletion or removal of their personal data in the following cases (subject to a number of exceptions):

- The data is no longer necessary for the purpose for which it was collected or otherwise processed.

- The data subject withdraws consent on which processing is being based and no other legal processing ground can be relied on.
- The data subject validly objects to the processing.
- The data has been unlawfully processed.
- The erasure is required for compliance with a legal obligation under EU or Member State law.
- Data has been collected in relation to the offer of information society services to a child.
- Personal data the company/organisation holds is needed to exercise the right of freedom of expression.
- There is a legal obligation to keep that data.
- Data is being held for reasons of public interest (for example, public health, scientific, statistical or historical research purposes).

Upon the individual's request, the data controller must delete that individual's personal data without undue delay and stop sharing it with third parties. If the data controller has made the personal data public, taking into account available technology and cost, it must also take reasonable steps to inform other data controllers that are processing the data of the requested erasure to ensure they can delete any copies of, or links to, such data. While also referred to as a "right to be forgotten," the right to erasure does not go as far as the right to be forgotten, as established by the EU Court of Justice in *Google Spain v Costeja*.

29 What is the right to restriction of processing? (Article 18)

A data subject has the right to restrict the processing of personal data in cases where:

- The accuracy of the data is contested by the data subject and the data controller is in the process of verifying the accuracy.
- The data processing is unlawful and the data subject requests the restriction of use rather than erasure of the data.
- The data controller no longer needs the data for the purposes of the processing, but the data is required by the individual regarding legal claims.
- The data subject objected to processing and the data controller is in the process of verifying whether it can rely on compelling legitimate grounds to continue the processing.

As long as a processing restriction applies, data controllers may store the relevant data but may no longer process it in any other way except with the data subject's consent, for the establishment, exercise or defence of legal claims, or for reasons of important public interest.

The GDPR does not prohibit profiling per se; rather, profiling is permitted as long as there is a legal basis for it (e.g., consent or legitimate interests) and individuals do not validly object to the profiling. Individuals have a broad right to object to profiling where it is undertaken for direct marketing purposes.

30 Are data controllers required to notify others of rectifications or erasures of data or processing restrictions? (Article 19)

Yes. Data controllers must communicate any correction or deletion of personal data or restriction of processing to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate efforts.

31 What is the right to data portability? (Article 20)

This is the right of the individual to receive personal data from a data controller in a structured, commonly used and machine-readable format and to transmit that data to another data controller without obstruction from the data controller to which the personal data has been originally provided. Individuals have the right to have the personal data transmitted directly from one data controller to another, where technically feasible. The right to data portability only applies where processing is carried out by automated means and is based on consent or a contract.

The right to data portability will be constrained to the extent that the exercise of such rights adversely impacts the rights and freedoms of others. Data controllers are encouraged to develop interoperable formats to enable data portability, but there is no obligation on controllers to adopt processing systems that are technically compatible.

32 What is the right to object? (Article 21)

Individuals have the right to object to processing in a number of circumstances, including the following:

- Processing occurs for direct marketing purposes.
- Processing is based on the legitimate interests of the data controller or a third party.

The right to object is outright in the context of direct marketing, meaning the data controller must stop to process the relevant data for direct marketing purposes when that right is exercised. In the second case above, the data controller must stop the data processing unless and until it demonstrates compelling legitimate grounds for the processing which override the interests and rights of the data subject.

33 What rights do data subjects have in relation to profiling and automated decision-making? (Article 22)

Profiling is essentially any automated data processing that involves the use of personal data to evaluate certain personal aspects of an individual, such as personal preferences, economic situation, health, interests, location or movement. A common example would be the tracking of web-browsing activities in order to predict purchasing behaviour.

The GDPR does not prohibit profiling per se; rather, profiling is permitted as long as there is a legal basis for it (e.g., consent or legitimate interests) and individuals do not validly object to the profiling. Individuals have a broad right to object to profiling where it is undertaken for direct marketing purposes. They have a narrower right to object to profiling undertaken for the purposes of legitimate interests or the performance of tasks carried out in the public interest or in the exercise of official authority.

The GDPR protects individuals by providing that they have a right not to be subject to a decision based solely on profiling (or other automated processing activities) which produces legal effects concerning them or similarly significantly affecting them. For example, an automated refusal of an online credit application or e-recruiting practices without human intervention would not be permissible. There are certain exemptions to this right, such as where the individual consented, or the decision is necessary for the entering into or performance of a contract between the data subject and the data controller.

DATA CONTROLLERS AND DATA PROCESSORS

34 What is a data controller and what is a data processor? (Article 4)

A data controller is the person that determines the purposes and means of the data processing. A data processor is the person that processes personal data on behalf of the data controller. Unlike the Directive, the GDPR imposes privacy compliance obligations directly not only on the data controller but also on the data processor.

35 What is the accountability principle (Article 24)?

The GDPR requires data controllers to implement appropriate technical and organisational measures and be able to demonstrate that data processing activities are compliant with the GDPR requirements ("accountability"). What measures will be appropriate in each case will depend on the nature, scope, context and purposes of the relevant processing, as well as the risks for rights and freedoms of individuals. This is a cumbersome and far-reaching obligation in practice and may best be discharged by implementing comprehensive privacy management programmes.

36 What are joint data controllers? (Article 26)

It is possible for more than one organisation to be a data controller in relation to any given processing activity. Where two or more controllers determine the means and purposes of processing, they are considered joint data controllers. Joint data controllers are required to allocate data protection compliance responsibilities between themselves in the form of a formal arrangement, which must reflect their respective roles vis-à-vis data subjects. A summary of the arrangement must be made available to data subjects.

37 Are data controllers and data processors not established in the EU required to appoint a representative? (Article 27)

Data controllers and processors who are not established in the EU must appoint a representative to the extent they target EU data subjects. Such representatives must be appointed in writing and be established in one of the Member States where the relevant data subjects are located.

However, note that appointing a representative is not required when:

- Processing is occasional, does not include large-scale processing of special categories of data or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or
- the data controller is a public authority or body.

The GDPR introduces significant new requirements for data processing agreements, which will likely require most data controllers and data processors to update their data processing contracts.

38 Is a representative the same thing as a DPO? (Article 27 and 37)

No. Requirements for and responsibilities of representatives are different from those for data protection officers. A representative essentially is a "service of process agent," that can be addressed instead of or in addition to the data controller or processor by supervisory authorities or data subjects. The DPO (see Questions 48-50), on the contrary, is likely positioned within the organisation (but can be an external person) whose main responsibility is advising the data controller or processor on their obligations under the GDPR and monitoring compliance.

39 What would an organisation have to do to be considered "offering goods or services" to EU data subjects?

Recital 23 provides some guidance on this question, stating that it should be ascertained whether it is apparent that the controller or processor envisages offering goods or services in more than one Member State. The mere accessibility of a website or email address is insufficient to ascertain such intention. However, the use of language or a currency generally used in a Member State with the possibility of ordering goods or services in that language points toward an intention to target EU data subjects in the sense of offering goods or services. The following questions may help in practice:

- **Domain Name:** Does your organisation have an EU-based domain name such as .de, .fr, .ie or .eu?
- **Language:** Does your organisation have, for example, a French or German version of its website?
- **Currency:** Does your organisation offer transactions in euros or another EU-based currency?
- **Content:** Does your website have referrals or testimonials from individuals in, say, Greece?

If the answer to any of these questions is yes, the GDPR may well apply to any relevant data processing.

40 Will data controllers and data processors be required to update their data processing agreements? (Articles 28 and 29)

The GDPR introduces significant new requirements for data processing agreements which will likely require most data controllers and

data processors to update their data processing contracts. Compared to the Directive, the GDPR is much more prescriptive as to what content the agreement must cover. For example, it will be necessary to add provisions requiring the processor to assist the data controller in complying with its data breach notification requirements and carrying out data protection impact assessments (DPIAs). Data controllers also need to oblige their data processors contractually (at the choice of the data controller) either to delete or to return all personal data upon completion of the services relating to such processing. Additionally, data processors should provide data controllers with all necessary information to validate compliance with obligations under Article 28, as well as allow for and contribute to compliance audits.

41 Who will be required to keep records of processing activities? (Article 30)

As a general rule, under the GDPR, data controllers and data processors (and, where applicable, their representatives) will be required to maintain detailed written records of processing activities and make them available to supervisory authorities upon request. This is an important cornerstone of the positive obligation to be able to demonstrate GDPR compliance. On a positive note, organisations will no longer be routinely required to notify supervisory authorities of their data processing activities, as was the case in most Member States under the Directive. In addition, organisations employing fewer than 250 people are exempt from this obligation, unless:

- The processing is likely to result in a risk to the rights and freedoms of data subjects (e.g., scoring, comprehensive monitoring, use of new technologies, etc.);
- the processing is not occasional; or
- the processing includes special categories of data (see Question 7) or personal data relating to criminal convictions and offences (see Question 8).

In practice, a substantial number of companies employing fewer than 250 people are still likely to be required to keep a record of processing activities.

42 What information should be maintained as a record of processing activity? (Article 30)

The processing record must be in writing (which includes electronic form) and contain detailed information. The GDPR distinguishes between data controllers and data processors in terms of what information must be recorded. Organisations would be well advised to refer to Article 30 and available guidance from supervisory authorities to understand their exact record-keeping obligations. Broadly, the GDPR requires that the following information be recorded:

- Details of the data controller, processor and any representative (if applicable)
- Purposes of the processing
- Categories of data subjects and categories of personal data
- Categories of recipients
- Details regarding cross-border transfers
- Data retention periods
- Description of technical and organisational security measures to safeguard the personal data

43 What security measures are required for data processing? (Article 32)

Under Article 32, both data controllers and data processors are required to implement appropriate technical and organisational measures to ensure a level of data security proportional to the risks inherent in the data processing for the rights and freedoms of individuals. This is a broad-brush obligation which, in practice, requires a detailed assessment of various factors, including the purposes of data processing activities, potential risks, state of the art of security, and implementation costs. Rather than prescribing specific security measures, the GDPR proposes some high-level options, namely:

- Pseudonymization or encryption
- The ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services based on recognised standards and appropriate to the level of risk of the organisation
- 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 testing, assessing and evaluating the effectiveness of security measures

Organisations may also wish to consider adhering to an approved code of conduct or obtaining certifications, as both may help demonstrate compliance with the security requirements under GDPR.

44 What do organisations need to do in the event of a data breach? (Articles 33 and 34)

The GDPR introduces a broad data breach notification obligation for data controllers which, under the Directive, only very few Member States had in place. Compliance with this obligation is crucial, as non-compliance can lead to substantial fines and reputational losses. While the obligation directly applies only to data controllers, data processors do have an obligation to notify data controllers without undue delay if they become aware of a data breach.

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

In the event of a data breach, data controllers must:

- Notify the breach to the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Subject to limited exceptions, communicate the breach to affected data subjects without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

A communication of the data breach to affected individuals is not required in the following circumstances (but data controllers should take care to ensure they can demonstrate such circumstances if they decide not to notify affected individuals):

- The data controller adequately secured the relevant data by implementing appropriate technical and organisational protection measures (such as encryption) in relation to it;
- following the breach, the data controller has taken measures to ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialise; or

- the notification of individual data subjects would require disproportionate effort — in this case, a public communication of the breach would be required, though.

The GDPR prescribes in Articles 33 and 34 what content any data breach notification must contain (e.g., specific information about the nature of the data breach, the likely consequences of the breach, the measures taken to mitigate the risks) and distinguishes between notifications to the supervisory authority and notifications to the affected individuals. In any event, what information to disclose in such notifications needs to be carefully considered.

The notification time frames prescribed by the GDPR are very short and require data controllers to give swift and maximal attention to any actual or suspected data breach. In practice, it may not always be clear when a data controller is "aware" of a breach. The Article 29 Working Party has issued guidance which suggests that a data controller is aware of a data breach when it "has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised." The guidance further states the following:

> "When, exactly, a data controller can be considered to be 'aware' of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required."

45 What is a data protection impact assessment and when is it required? (Article 35)

A data protection impact assessment (DPIA) is a formal, systematic process to assess the impact of any envisaged processing operations on the protection of personal data. A DPIA is required by the GDPR in specific situations, with the goal of minimising risks to the rights and freedoms of data subjects. The assessment should be undertaken by the data controller prior to starting a relevant personal data processing activity.

A data protection impact assessment is required by the GDPR in specific situations, with the goal of minimising risks to the rights and freedoms of data subjects.

A DPIA is compulsory when "a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in high risk to the rights and freedoms of natural persons." The GDPR lists the following examples in which case a DPIA would be required:

- Automated processing for purposes of profiling and similar activities intended to evaluate personal aspects of data subjects
- Processing on a large scale of special categories of data or of data relating to criminal convictions and offences.
- Systematic monitoring of a publicly accessible area on a large scale

Supervisory authorities are also expected to publish lists of processing operations, which will require a DPIA. Further, the Article 29 Working Party has issued useful guidance as to when a DPIA will likely need to be carried out in practice and recommends that, if in doubt, a DPIA should be carried out.

46 How do I carry out a DPIA and what information must any DPIA documentation include?

The GDPR does not prescribe a process or format for undertaking a DPIA. Rather, it is intended to provide flexibility to data controllers. The Article 29 Working Party Guidance (which should be consulted for further guidance in practice) confirms that data controllers may choose a methodology that suits their purposes on DPIAs.

However, the GDPR does prescribe the following minimum features of a DPIA:

- A description of the envisaged processing operations and the purposes of the processing
- An assessment of the necessity and proportionality of the processing
- An assessment of the risks to the rights and freedoms of data subjects
- The measures envisaged to address the risks (including safeguards, security measures and mechanisms to protect personal data) and demonstrate compliance with the GDPR

47 If the DPIA indicates a high risk to the rights/freedoms of data subjects, what additional actions must a data controller take prior to processing? (Article 36)

The data controller must consult the competent supervisory authority prior to an intended processing if a DPIA indicates that the intended data processing would result in a high risk in the absence of mitigating measures taken by the data controller. As part of the consultation process, the data controller must provide detailed information to the supervisory authority. As a general rule, the supervisory authority must respond within eight weeks of receiving the request for consultation and confirm whether the intended processing would infringe on the GDPR. But this period may be extended.

48 Is my organisation required to designate a data protection officer? (Article 37)

The GDPR requires both data controllers and data processors to appoint a DPO in any of the following cases:

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity.
- The core activities of the data controller or the processor consist of processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale.
- The core activities of the data controller or the data processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

Importantly, Member States may introduce requirements to appoint a DPO in cases that go beyond the above, so national legislation must be considered as well. By way of example only, Germany has more stringent requirements and it is more likely that organisations whose core activities are in Germany will have to appoint a DPO than, say, those that are based in the UK.

The Article 29 Working Party provides the following guidance that helps establish whether a DPO must be appointed in practice:

- "Core activities" include key operations necessary to achieve the business goals and activities inextricably linked to the core activities (e.g., processing patients' data is inextricably linked to a hospital's core activity of providing health care).
- "Large scale" should be determined on a case-by-case basis, considering the number of data subjects, the volume of data and/or the range of different data items, the duration, and geographical extent of processing.

- "Regular monitoring" is interpreted to mean ongoing or occurring at particular intervals for a particular period, recurring or repeated at fixed times, or constantly or periodically.
- "Systematic monitoring" indicates monitoring occurs according to a system; is pre-arranged, organised or methodical; is part of a general plan for data collection; or is carried out as part of a strategy.

Enterprises may appoint a single DPO for multiple entities so long as the DPO can be easily accessed. And they may choose whether to appoint an internal or an external DPO. DPOs must have the expert knowledge of data protection laws and practices to be able to fulfill their tasks.

49 To whom should the DPO report? (Article 38)

DPOs are to be assured independence in the performance of their tasks and shall directly report to the organisation's "highest management level." They may not be dismissed or penalised for performing their tasks and must be given the resources necessary to perform their tasks.

50 What are responsibilities of the DPO? (Article 39)

DPO responsibilities include:

- Informing and advising the controller/processor and employees who process personal data of their obligations to comply with the GDPR and other data protection laws
- Monitoring organisational compliance with the GDPR, other data protection laws and internal policies, including the assignment of responsibilities, awareness-raising, training of staff and internal audits
- Providing advice when requested regarding data protection impact assessments
- Cooperating with the supervisory authority and acting as the point of contact

DPOs are to be assured independence in the performance of their tasks and shall directly report to the organisation's "highest management level."

51 How are codes of conduct used under the GDPR? (Article 40)

The GDPR encourages the development of codes of conduct to assist with the proper application of the regulation. Such codes of conduct are expected to provide guidance and best practices in specific processing contexts in various sectors. Adherence to such codes of conduct will help data controllers and data processors demonstrate compliance with the GDPR.

The GDPR authorises associations and other bodies representing categories of data controllers or data processors to prepare such codes. These codes then need to be approved by a supervisory authority, or the EDPB in the case of cross-Member State relevance.

The GDPR lists the following topics for codes of conduct:

- Fair and transparent processing
- Legitimate interests pursued by controllers in specific contexts
- The collection of personal data
- The pseudonymization of personal data
- Information provided to the public and to data subjects
- The exercise of the rights of data subjects

- Information provided to, and the protection of, children and the obtaining of parental consent
- Obligations of data controllers, including privacy by design/default and measures to ensure the security of processing
- The notification of personal data breaches
- The transfer of personal data to third countries or international organisations
- Out-of-court proceedings along with other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to the processing

52 How will code of conduct compliance be enforced? (Article 41)

Bodies that have the appropriate expertise in relation to the subject matter of a code of conduct and demonstrate independence may be accredited, in which case they will have the power to monitor compliance with codes of conduct. Data controllers and data processors that are found to be incompliant with a relevant code may be suspended from participation in the code and reported to supervisory authorities.

53 What is required for accreditation? (Article 41)

In order to be accredited by the competent supervisory authority to monitor compliance with a code of conduct, a body must:

- Demonstrate its independence and expertise in relation to the subject matter of the code.
- Establish procedures which allow it to assess the eligibility of controllers and processors to apply the code, to monitor their compliance with its provisions and to periodically review its operation.
- Establish procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public.
- Demonstrate to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interest.

54 What are certifications? (Articles 42 and 43)

The GDPR encourages Member States, supervisory authorities, the EDPB and the European Commission to establish data protection certification mechanisms and data protection seals and marks. Certification will be voluntary but will enable data controllers and processors to demonstrate GDPR compliance, particularly regarding the implementation of appropriate technical and organisational measures. They will also be helpful in the context of data transfers to third countries outside the EU, as data controllers and data processors outside the EU may rely on them for the purpose of demonstrating appropriate safeguards.

Certifications will be issued by accredited certifying bodies or the competent supervisory authority on the basis of established criteria and will be valid for a maximum period of three years once issued. They may be renewed under the same conditions. Certification will be withdrawn where the requirements for certification are no longer met.

The EDPB is tasked with collating and making publicly available all certification mechanisms and data protection marks and seals.

CROSS-BORDER DATA TRANSFERS

55 What is the basic rule for cross-border data transfers?

The GDPR largely retains the cross-border transfer rules established under the Directive. As a general rule, personal data may only be transferred out of the EU/EEA to countries which have been recognised as providing an adequate level of data protection ("adequacy decision"). Data may only be transferred to other non-EU/EEA countries if the transferor can rely on specific derogations or adduces specific additional safeguards ensuring an adequate level of data protection.

56 What is an adequacy decision with regard to cross-border data transfer? (Article 45)

The European Commission has the power to conclude that any given country outside the EU/EEA ("third country"), or a territory or one or more specified sectors within that third country, or an international organisation ensures an adequate level of data protection by issuing an adequacy decision. Data transfers to these countries, territories, sectors or organisations which have been given adequacy status are permitted, without any further specific authorisation, by supervisory authorities.

At the time of this writing, such "adequate" jurisdictions include Andorra, Argentina, Canada (commercial organisations subject to PIPEDA), the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. Japan is in the process of agreeing on mutual adequacy findings with the Commission.

In relation to the United States, the Commission issued an adequacy decision in July 2016 with respect to the Privacy Shield Framework. Under the Privacy Shield, U.S. organisations may self-certify to the U.S. Department of Commerce and publicly commit to comply with the framework's privacy standards recognised by the Commission as essentially equivalent to the EU privacy standards. Thus, the Privacy Shield

enables data transfers for commercial purposes from the EU to U.S. organisations that participate in the Privacy Shield. Self-certification is voluntary but once an organisation makes the public commitment to comply with the framework's requirements, the commitment will become enforceable under U.S. law.

As a general rule, personal data may only be transferred out of the EU/EEA to countries which have been recognised as providing an adequate level of data protection.

While the GDPR retains the adequacy concept introduced by the Directive, it brings noteworthy changes, including the following:

- Adequacy decisions may be made not only in relation to a country but also in relation to territories, sectors and international organisations.
- Adequacy decisions will be subject to periodic review and may be repealed, amended or suspended by the Commission.
- The conditions for an adequacy decision are stricter. For instance, in order to be awarded adequacy status, a third country needs to ensure a level of data protection *essentially equivalent* to that guaranteed within the EU. In particular, it must ensure effective independent data protection supervision and data subjects must be provided with effective and enforceable rights and effective administrative and judicial redress.

The stricter additional requirements for adequacy decisions stem from the infamous *Schrems decision* which led to the invalidation of Safe Harbour and the implementation of the Privacy Shield.

57 What are considered appropriate safeguards under the GDPR? (Article 46)

Data transfers from the EU to third countries that do not enjoy adequacy status are nonetheless permissible if the transferor adduces specific additional safeguards ensuring an adequate level of data protection and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The GDPR provides for appropriate safeguards that do not require specific authorisation from a supervisory authority and those that do require such authorisation.

The following appropriate safeguards do not require specific supervisory authority authorisation:

- Binding corporate rules (See Question 58)
- Standard data protection clauses adopted by the Commission (See Question 59)
- Approved codes of conduct or approved certification mechanisms, in each case together with binding and enforceable commitments of the controller/processor in the third country to apply the appropriate safeguards, including with regard to data subjects' rights (See Questions 51–54)
- Legally binding and enforceable instruments between public authorities or bodies

Appropriate safeguards that do require specific authorisation from the supervisory authority are:

- Contractual clauses between the controller or processor on the one hand, and the controller, processor or recipient of the data in the third country or international organisation on the other hand
- Provisions to be inserted into administrative agreements between public authorities or bodies which include enforceable and effective data subject rights

58 What are binding corporate rules? (Article 47)

Binding corporate rules (BCRs) are a set of binding rules or codes of conduct which multinational organisations may choose to draft and implement within the organisation in order to legitimise cross-border data transfers within their corporate group. BCRs impose EU privacy standards on an organisation's affiliates outside the EU in order to allow those affiliates to process data originating from the EU. BCRs cannot be used to legitimise transfers to non-affiliated entities such as suppliers, customers, distributors or service providers. BCRs are quite cumbersome to put in place but the GDPR strives to ease that compliance burden. BCRs require approval from the competent supervisory authority.

59 What are standard data protection clauses? (Article 46)

Standard data protection clauses (also referred to as "model clauses") are another way of adducing appropriate safeguards in the context of data transfers from the EU to third countries without adequacy status. The model clauses impose obligations on both the transferor and the transferee of the data to ensure that the transfer arrangements protect the rights and freedoms of the data subjects. Where data controllers or data processors use the model clauses in their entirety and in an unaltered way, they will have adduced appropriate safeguards for the relevant data transfer.

Pre-GDPR, the Commission issued standard contractual clauses for data transfers from EU data controllers to non-EU data controllers, as well as standard contractual clauses for data transfers from EU controllers to non-EU processors. These will remain in force under the GDPR unless and until formally repealed, amended or replaced. Under the GDPR, standard data protection clauses may be adopted by the Commission or adopted by a supervisory authority and then approved by the Commission.

Importantly, under the GDPR, data controllers or data processors may supplement approved standard contractual clauses with additional clauses or safeguards as long as these do not contradict the approved standard contractual clauses or prejudice the fundamental rights and freedoms of the data subjects. Standard data protection clauses as a means of legitimising cross-border data transfers are currently under challenge before the Court of Justice of the European Union.

Standard data protection clauses are another way of adducing appropriate safeguards in the context of data transfers from the EU to third countries without adequacy status.

60 What are the derogations for cross-border data transfers that can be relied upon under the GDPR? (Article 49)

Data transfers to third countries without adequacy status may also be legitimate if the transferor can rely on specific derogations. Under the GDPR, available derogations are:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.

- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- The transfer is made from a public register and specific conditions are met.
- The transfer is not repetitive, concerns only a limited number of data subjects and is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller adduces suitable safeguards to protect the personal data and informs the supervisory authority and the data subjects about the transfer.

The last derogation has been newly introduced by the GDPR and should be seen as a "last resort" derogation that may legitimise occasional data transfers concerning only a small number of data subjects.

SUPERVISORY AUTHORITIES

61 Will Member States still have national supervisory authorities under the GDPR? (Article 51)

Yes. Each Member State is required to provide for one or more independent public authorities to be responsible for monitoring the application of the GDPR. Most Member States will continue to have one such national supervisory authority. Some Member States (e.g., Germany) will have several supervisory authorities. These Member States will be required to designate the supervisory authority which is to represent those authorities in the EDPB and set out a mechanism to ensure compliance by the various authorities with the consistency mechanism (see Question 66).

62 Which supervisory authority has jurisdiction in the case of cross-border processing cases? (Article 56)

Each supervisory authority has jurisdiction to act on its own territory. Without qualifications, this rule would frequently lead to multiple supervisory authorities having jurisdiction to act on the same matter where a data controller engages in cross-border processing either through multiple establishments or otherwise (e.g., because data subjects are located in various Member States). To safeguard controllers and processors from having to deal with multiple supervisory authorities, Article 56 provides that the supervisory authority of the main or single establishment of the data controller/processor will have jurisdiction to act as "lead" supervisory authority for the cross-border processing carried out by that controller. But the lead supervisory authority is under an obligation to cooperate with other "concerned" supervisory authorities. Such other concerned supervisory authorities would be those in other countries where the data controller or processor might be established, where affected data subjects are located or those that have received complaints. In practice, it can be difficult to identify the lead supervisory authority. The Article 29 Working Party has issued guidelines which should be consulted.

This rule for cross-border processing is also subject to important derogations. For instance, a supervisory authority other than the lead authority will have jurisdiction to handle a complaint lodged with it or a possible infringement of the GDPR if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State. So, there will be room for local supervisory authorities to argue that they will have jurisdiction even though they are not the lead supervisory authority.

While the Commission originally intended to create a one-stop-shop system, whereby businesses operating in multiple EU countries should only have to deal with one supervisory authority, in practice, owing to amendments introduced into the Commission's draft legislation as it went through the process of enactment, this will frequently not be the case.

63 What are the rules for cooperation between the lead supervisory authorities and concerned authorities? (Articles 60-62 and 66)

The GDPR sets out detailed rules for the cooperation between the lead and concerned supervisory authorities, including that they are required to exchange information, the concerned supervisory authorities shall provide assistance to the lead authority upon request (such as conducting investigations) and the lead authority shall seek input on draft decisions from concerned authorities. Where supervisory authorities cannot reach agreement on relevant matters, the matters will be referred to the EDPB for resolution.

This cooperation requirement is subject to an urgency exception. A concerned supervisory authority may immediately adopt provisional measures intended to produce legal effects on its own territory and valid for no more than three months if it has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects (e.g., because otherwise the enforcement of a right of a data subject could be considerably impeded).

64 What responsibilities are assigned to the supervisory authority? (Article 57)

Supervisory authorities have a long list of tasks listed in Article 57. First and foremost, they are responsible for monitoring and enforcing the application of the GDPR; promoting awareness and understanding of the risks, rules, safeguards and rights in relation to personal data processing; handling complaints; encouraging the drawing up of codes of conduct; and providing advice on data processing operations.

65 What are supervisory authority action reports? (Article 59)

Each supervisory authority is required to publish an annual report on its activities, which may include a list of types of infringement notified and types of measures taken. These reports will be made public and will likely provide useful insights into regulator enforcement behaviour and priorities.

66 What is the consistency mechanism? (Articles 63-67)

The GDPR requires cooperation between the various national supervisory authorities and, where relevant, with the Commission to ensure a consistent application throughout the EU. The EDPB will play an important role in promoting consistency by issuing opinions and guidance, reporting to the Commission, and resolving disputes between supervisory authorities. Further, supervisory authorities must obtain the EDPB's opinion before they adopt any of the measures listed in Article 64, such as binding corporate rules, standard contractual clauses or lists of processing operations that fall under the DPIA requirement. In cases of conflict, the EDPB has the last word.

REMEDIES, LIABILITIES AND PENALTIES

67 How may a data subject lodge a complaint? (Article 77)

Data subjects have the right to file complaints with a supervisory authority if they consider that the processing of personal data relating to them infringes the GDPR. The complaint may be lodged with the supervisory authority in the Member State where the data subject resides or works or where the alleged infringement took place. Within 90 days of the complaint, the supervisory authority is required to inform the data subject regarding the complaint's status.

68 May data subjects also start court proceedings? (Articles 78 and 79)

Yes. Without prejudice to the right to file a complaint with the supervisory authority, each data subject also has the right to an effective judicial remedy where they consider that their rights have been infringed as a result of the processing of their personal data in non-compliance with the GDPR. Such proceedings against data controllers or data processors are to be brought before the courts of the Member State where the data controller or processor has its place of establishment or where the data subject has its habitual place of residence.

Further, data subjects have a right to an effective judicial remedy against a legally binding decision of a supervisory authority or in cases where the supervisory authority does not handle a complaint or does not inform the complainant appropriately of the progress of the complaint. Such proceedings are to be brought before the courts of the Member State where the supervisory authority is established.

69 Can data subjects receive compensation for infringements? (Article 82)

Yes. Any person who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to receive compensation from the data controller or data processor for damage suffered. Both controllers and processors may be held liable for the damage caused. Controllers involved in processing will be liable for any damage caused by processing that infringes the GDPR. Processors will only be liable for damage caused by processing where they have not complied with the GDPR obligations specifically directed to processors or where they have acted outside or contrary to lawful instructions of the controller. Both controllers and processors are exempt from liability if they prove that they are not in any way responsible for the event giving rise to the damage.

70 Must data controllers and data processors fear administrative fines and penalties under the GDPR?

The GDPR expressly states that as a general rule (in order to strengthen enforcement of the GDPR rules), penalties and administrative fines should be imposed for any infringement of the GDPR in addition to, or instead of, appropriate measures imposed by the supervisory authority. The exceptions are minor infringements and cases in which a fine would constitute a disproportionate burden to a natural person. In those cases, a reprimand may be issued instead. The GDPR sets the upper limit and criteria for determining fines, which are then finally determined by the competent supervisory authority in each individual case.

71 How will it be determined whether an administrative fine will be imposed, and if so, how will the amount of the fine be determined? (Article 83)

As a general rule, supervisory authorities must ensure that the imposition of administrative fines is effective, proportionate and dissuasive in each case. Article 83 contains a comprehensive list of factors which must be considered when deciding whether to impose a fine and deciding on the amount of the fine. These include:

- The nature, gravity and duration of the infringement
- The intentional or negligent character of the infringement
- Action taken to mitigate the damage suffered
- Degree of controller/processor responsibility
- Any relevant previous infringements by the controller/processor
- The degree of cooperation with the DPA
- Categories of data involved in the infringement
- The manner in which the infringement became known to the supervisory authority
- Degree of compliance with previous corrective orders on the same subject matter
- Adherence to approved codes of conduct or certification mechanisms
- Other aggravating/mitigating factors relevant to the case

The GDPR provides for two different levels of fines. In each case, the GDPR sets the upper limit and the competent supervisory authority determines the amounts in each case having regard to the factors listed above.

Infringements of the following provisions are subject to administrative fines of up to €10 million, or in the case of an undertaking, up to 2 percent of the worldwide annual turnover of the preceding financial year (whichever is higher).

Article 8 – Conditions applicable to child's consent in relation to information society services
Article 11 – Processing which does not require identification
Article 25 – Data protection by design and by default
Article 26 – Joint controllers
Article 27 – Representatives of controllers or processors not established in the Union
Article 28 – Processor
Article 29 – Processing under the authority of the controller or processor
Article 30 – Records of processing activities
Article 31 – Cooperation with the supervisory authority
Article 32 – Security of processing
Article 33 – Notification of a personal data breach to the supervisory authority
Article 34 – Communication of a personal data breach to the data subject
Article 35 – Data protection impact assessment
Article 36 – Prior consultation
Article 37 – Designation of the data protection officer
Article 38 – Position of the data protection officer
Article 39 – Tasks of the data protection officer
Article 40 – Codes of conduct
Article 41 – Monitoring of approved codes of conduct
Article 42 – Certification
Article 43 – Certification bodies

Infringements of the following provisions are subject to administrative fines of up to €20 million, or in the case of an undertaking, up to 4 percent of the worldwide annual turnover of the preceding financial year (whichever is higher).

Article 5 – Principles relating to processing of personal data
Article 6 – Lawfulness of processing
Article 7 – Conditions for consent
Article 9 – Processing of special categories of personal data
Article 10 – Processing of personal data relating to criminal convictions and offences
Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject
Article 13 – Information to be provided where personal data are collected from the data subject
Article 14 – Information to be provided where personal data have not been obtained from the data subject
Article 15 – Right of access by the data subject
Article 16 – Right to rectification
Article 17 – Right to erasure ("right to be forgotten")
Article 18 – Right to restriction of processing
Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing
Article 20 – Right to data portability
Article 21 – Right to object
Article 22 – Automated individual decision-making, including profiling
Article 44 – General principle for transfers
Article 45 – Transfers on the basis of an adequacy decision
Article 46 – Transfers subject to appropriate safeguards
Article 47 – Binding corporate rules
Article 48 – Transfers or disclosures not authorised by Union law
Article 49 – Derogations for specific situations
Article 58 – Supervisory authority powers

SOME SPECIFIC PROCESSING SITUATIONS

72 Does the GDPR apply to data processing in the employment context? (Article 88)

Yes. The GDPR applies, but Article 88 allows Member States to provide more specific rules to ensure the protection of data in the employment context. This means that each Member State may establish their own rules for processing of data in the employment context. Therefore, multinational employers will need to understand and adhere to the national rules in each case.

The GDPR also states that employee consent to the processing of their personal data is unlikely to be valid as it is unlikely to be freely given.

73 Does the GDPR limit the processing of data for research purposes? (Article 89)

The processing of personal data for scientific or historical research purposes is permitted, provided appropriate safeguards (e.g., pseudonymization) are in place. Scientific research is to be interpreted broadly and includes, for example, technological development and demonstration, fundamental research, applied research, and privately funded research.

74 Does the GDPR override professional secrecy obligations? (Article 90)

Where controllers or processors are subject to obligations of professional secrecy, such obligations may conflict with powers of supervisory authorities to request access to data or premises. The GDPR recognises this and allows Member States to introduce specific rules to set out the powers of supervisory authorities to reconcile the right of protection of personal data with the obligation of secrecy.

ABOUT BAKER MCKENZIE

Baker McKenzie helps clients overcome the challenges of competing in the global economy. We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instil confidence in our clients. (www.bakermckenzie.com)

ABOUT ROBERT HALF

Founded in 1948, Robert Half is the world's first and largest specialised staffing firm and a recognised leader in professional consulting and staffing services. The company's professional staffing services include: Accountemps®, Robert Half® Finance & Accounting and Robert Half® Management Resources, for temporary, full-time and senior-level project professionals, respectively, in the fields of accounting and finance; OfficeTeam®, for highly skilled office and administrative support professionals; Robert Half® Technology, for information technology professionals; Robert Half® Legal, for temporary, project and full-time staffing of attorneys, paralegals and legal support professionals and consulting solutions; and The Creative Group®, for interactive, design, marketing, advertising and public relations professionals.

Robert Half also is the parent company of Protiviti®, a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. For more information, including career resources and industry research, visit roberthalf.com.

ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

For more information, go to: protiviti.com/GDPR

HOW PROTIVITI HELPS COMPANIES SUCCEED

In a world where business and technology are inextricably interconnected, security can no longer be viewed as supplemental to business. Our mission is to help executives across all industries design security and privacy systems that not only protect the business but also unlock revenue growth opportunities in a true business-IT partnership. We offer a full spectrum of security and privacy assessment, architecture, transformation and management services:

- Security Programme and Strategy
- Vulnerability Assessment and Penetration Testing
- Incident Response and Forensics Services
- Data Security and Privacy Management
- Identity and Access Management
- Cybersecurity Intelligence Response Center (CIRC)

CONTACTS

BAKER MCKENZIE

UNITED KINGDOM

Harry Small
Partner
harry.small@bakermckenzie.com

AUSTRALIA

Anne-Marie Allgrove
Partner
anne-marie.allgrove@bakermckenzie.com

THE NETHERLANDS

Wouter Seinen
Partner
wouter.seinen@bakermckenzie.com

UNITED STATES

Brian Hengesbaugh
Partner
brian.hengesbaugh@bakermckenzie.com

FRANCE

Yann Padova
Partner
yann.padova@bakermckenzie.com

GERMANY

Michael Schmidl
Partner
michael.schmidl@bakermckenzie.com

HONG KONG

Paolo Sbuttoni
Partner
paolo.sbuttoni@bakermckenzie.com

SINGAPORE

Anne Petterd
Partner
anne.petterd@bakermckenzie.com

ITALY

Francesca Gaudino
Partner
francesca.gaudino@bakermckenzie.com

SPAIN

Raul Rubio
Partner
raul.rubio@bakermckenzie.com

ROBERT HALF

Joel Wuesthoff
Managing Director
Robert Half Legal
joel.wuesthoff@roberthalflegal.com

Jeffrey Weber
Executive Director
Robert Half Technology
jeffrey.weber@roberthalf.com

PROTIVITI

UNITED STATES

Ron Lefferts
Managing Director
Global Leader, Technology Consulting Practice
ron.lefferts@protiviti.com

Scott Laliberte
Managing Director
scott.laliberte@protiviti.com

Andrew Retrum
Managing Director
andrew.retrum@protiviti.com

Jeff Sanchez
Managing Director
jeffrey.sanchez@protiviti.com

Cal Slemp
Managing Director
cal.slemp@protiviti.com

Michael Walter
Managing Director
michael.walter@protiviti.com

Diana Candela
Associate Director
diana.candela@protiviti.com

AUSTRALIA

David Adamson
Managing Director
david.adamson@protiviti.com.au

FRANCE

Nuvin Goonmeter
Managing Director
nuvin.goonmeter@protiviti.fr

GERMANY

Kai-Uwe Ruhse
Managing Director
kaiuwe.ruhse@protiviti.de

HONG KONG

Michael Pang
Managing Director
michael.pang@protiviti.com

ITALY

Enrico Ferretti
Managing Director
enrico.ferretti@protiviti.it

UNITED KINGDOM

Thomas Lemon
Managing Director
thomas.lemon@protiviti.co.uk

PROTIVITI GLOBAL MARKET LEADERS

ARGENTINA

Pablo Giovannelli
+54.11.5278.6345
pablo.giovannelli@protivitiglobal.com.pe

AUSTRALIA

Garran Duncan
+61.3.9948.1200
garran.duncan@protiviti.com.au

BAHRAIN

Arvind Benani
+973.1.710.0050
arvind.benani@protivitiglobal.me

BRAZIL

Raul Silva
+55.11.2198.4200
raul.silva@protivitiglobal.com.br

CANADA

David Dawson
+1.647.288.4886
david.dawson@protiviti.com

CHILE

Soraya Boada
+56.22.573.8580
soraya.boada@protivitiglobal.cl

CHINA (HONG KONG)

Albert Lee
+852.2238.0499
albert.lee@protiviti.com

CHINA (MAINLAND)

David Cheung
+86.21.5153.6900
david.cheung@protiviti.com

FRANCE

Bernard Drui
+33.1.42.96.22.77
drui@protiviti.fr

GERMANY

Michael Klinger
+49.69.963.768.155
michael.klinger@protiviti.de

INDIA

Sanjeev Agarwal
+91.124.661.8600
sanjeev.agarwal1@protivitiglobal.in

ITALY

Alberto Carnevale
+39.02.6550.6301
alberto.carnevale@protiviti.it

JAPAN

Yasumi Taniguchi
+81.3.5219.6600
yasumi.taniguchi@protiviti.jp

KUWAIT

Sanjeev Agarwal
+965.2242.6444
kuwait@protivitiglobal.me

MEXICO

Roberto Abad
+52.55.5342.9100
roberto.abad@protivitiglobal.com.mx

NETHERLANDS

Anneke Wieling
+31.20.346.0400
anneke.wieling@protiviti.nl

OMAN

Shatha Al Maskiry
+968 24699402
shatha.maskiry@protivitiglobal.me

PERU

Marco Villacorta
+51.1.208.1070
marco.villacorta@protivitiglobal.com.pe

QATAR

Andrew North
+974.4421.5300
andrew.north@protivitiglobal.me

SAUDI ARABIA

Saad Al Sabti
+966.11.2930021
saad.alsabti@protivitiglobal.me

SINGAPORE

Sidney Lim
+65.6220.6066
sidney.lim@protiviti.com

UNITED ARAB EMIRATES

Arindam De
+9714.438.0660
arindam.de@protivitiglobal.me

UNITED KINGDOM

Peter Richardson
+44.20.7930.8808
peter.richardson@protiviti.co.uk

UNITED STATES

Scott Laliberte
+1.267.256.8825
scott.laliberte@protiviti.com

VENEZUELA

Gamal Perez
+58.212.418.46.46
gamal.perez@protivitiglobal.com.ve

bakermckenzie.com

roberthalf.com

protiviti.com