FAEGRE BAKER DANIELS

The EU General Data Protection Regulation: Practical Implications for U.S. Businesses

TABLE OF CONTENTS

PAGE 3 Introduction

PAGE 4 Territorial Scope

PAGE 5 Appointment of a Representative

PAGE 6 Appointment of a Data Protection Officer

PAGE 7 Information Requirements and Privacy Notices

PAGE 8 Records of Processing Activities

PAGE 9 Requirements for Consent

PAGE 10 Legitimate Interest

PAGE 10 New and Enhanced Rights 1: Right to Object

PAGE 11 New and Enhanced Rights 2: Automated Decisions and Profiling

PAGE 12 New and Enhanced Rights 3: Right to Data Portability

PAGE 12 New and Enhanced Rights 4: Right to Erasure (Right to be "Forgotten")

PAGE 13 New and Enhanced Rights 5: Right to Restrict Processing

PAGE 13 Data Protection by Design and Default

PAGE 14 Technological and Organisational Changes

PAGE 15 Data Security and Breach Notification

PAGE 16 Vendor Management

PAGE 17 Sanctions

PAGE 18 International Data Transfers

PAGE 19 Key Contacts

INTRODUCTION

From 25 May 2018, radical changes to data privacy laws in the European Union will come into effect. Businesses should start preparing now, given the significant changes. The General Data Protection Regulation (GDPR) will impact U.S. businesses, regardless of whether they have a corporate presence in the EU or use EU based assets to process data (which are the current tests). If a U.S. business offers goods or services to EU based customers, or monitors their behaviour, for example through data analytics, they will potentially be within the scope of the GDPR.

The extra-territorial reach means that in practice, many businesses operating internationally will need to adopt European data privacy standards, which are likely to become the default global standards. The increased sanctions under the GDPR (up to a headline grabbing 4 percent of global revenue), together with general public expectations on data privacy, means that compliance with data privacy laws cannot be treated as a minor regulatory issue. The level of fines and other penalties puts data privacy at the same level as antitrust or anti-bribery and corruption compliance on the corporate compliance agenda. This will require board level awareness and leadership and the combined input from a range of professionals including, legal, IT, finance, procurement and vendor management and HR.

In particular, the GDPR:

- Introduces new rights that may require changes to:
  - Privacy policies
  - Internal procedures
  - Technology platforms
  - Vendor agreements
- Introduces new obligations covering:
  - Requirements for consent
  - Data breach notification
  - Appointment of third party data processors
  - Appointment of representatives
- Requires new processes including:
  - Privacy Impact Assessments
  - Internal record-keeping/audit trail
  - Privacy by design and default
  - Implementing robust data security measures (e.g., pseudonymization and anonymization)
- Potentially requires hiring new personnel (or re-assignment of existing personnel) as a Data Protection Officer
- Has significant penalties for non-compliance (up to €20,000,000 or 4 percent of worldwide annual turnover for the most serious breaches)

The GDPR is intended to provide much greater harmonization than at present, although some differences will remain. Some areas, notably personal data relating to employees, remain subject to significant national variances. The United Kingdom will adopt the GDPR, despite its planned withdrawal from the EU in 2019. This reflects the fact that a high level of protection for personal data is expected in many modern economies and the global trend towards higher levels of protection. In particular it provides a firmer basis for the U.K. to be recognized by the EU as offering an adequate level of protection for international transfers of personal data.

This guide sets out some of the key areas which are relevant to U.S. businesses. The GDPR has had a long and convoluted legislative history and is one of the most heavily lobbied pieces of European legislation ever. It is comprised of 99 Articles, 173 Recitals and was subject to 3,999 amendments and the text below is a brief summary of its complex provisions. For further information, please contact a member of our team listed below.

TERRITORIAL SCOPE

Summary

The GDPR applies to:

- Organisations with EU businesses which process data as part of their EU establishment
- The processing of personal data by a controller or processor which is not in the EU if it:
  - Offers goods or services to data subjects that are in the EU or
  - Monitors their behaviour in the EU

Changes to the Directive

The GDPR has significant extra-territorial reach. Currently a U.S. business only needs to comply with EU data protection laws where data processing is carried out as part of its European establishment or where it uses data processing equipment located in the EU. Under the GDPR, a U.S. company without a business presence in the EU, but which markets to EU based consumers or monitors their behaviour, will potentially be subject to the GDPR.

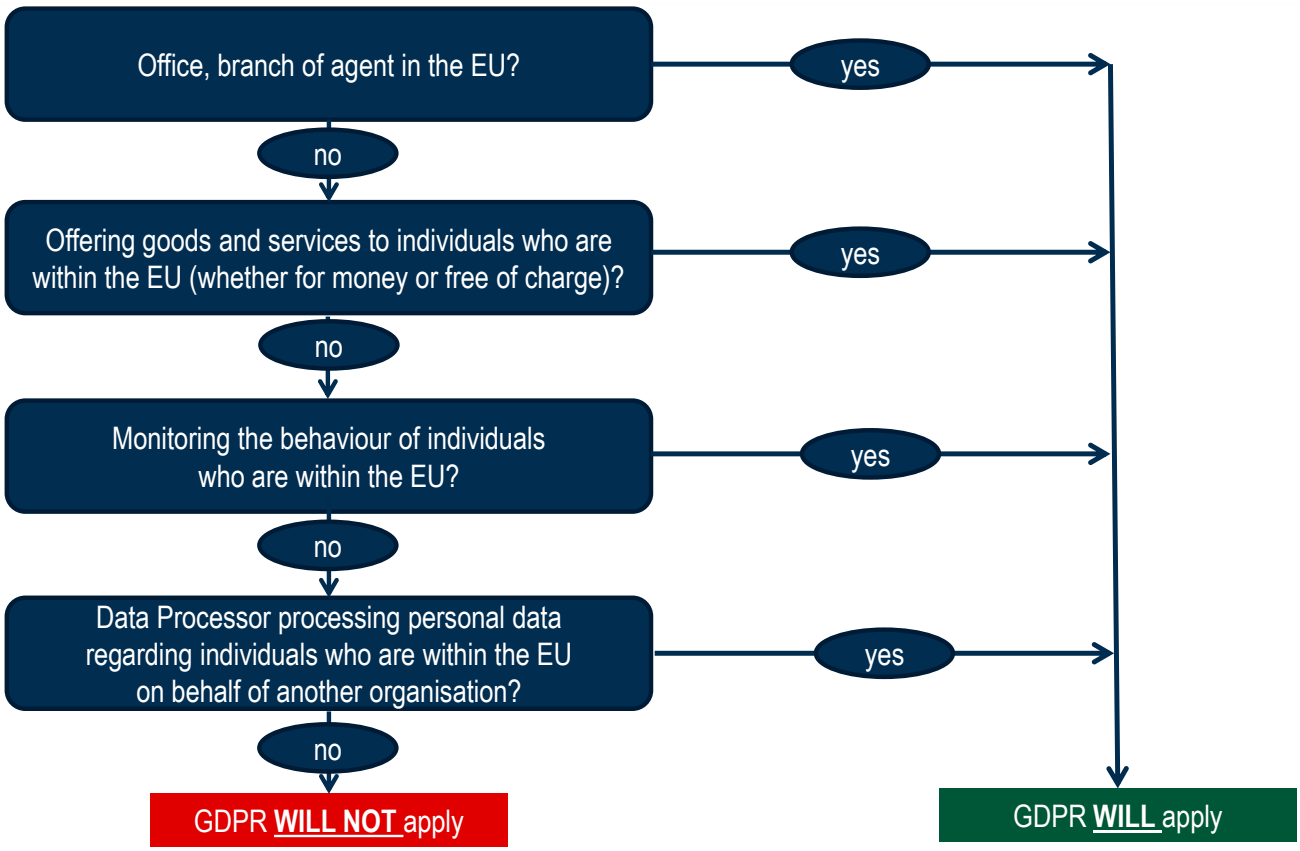
Furthermore, the Data Protection Directive applied to the data processing activities of a data controller (i.e., the business which decides on the purposes of processing and the means by which the processing is carried out). The GDPR extends this to data processors who process data on behalf of a customer.

Practical Implications

The widened scope means a vast range of U.S. businesses who previously did not need to comply will now be within the full scope of European data privacy law. For example, businesses that offer online services from the U.S. will be caught if they are processing data of EU customers in the course of offering goods or services to them. The precise reach of these provisions is still somewhat unclear, but they are more likely to be triggered if, for example, goods or services are offered in a local language or currency. The GDPR's concept of monitoring behaviour could encompass the use of cookies or other devices used to track online behaviour or location and/or analyse or predict personal preferences, attitudes and behaviours (e.g., customer profiling).

As a result, businesses that rely on targeted behavioral advertising and other data analytics are likely to be within the scope of the GDPR. Further, since both data controllers and data processors are subject to the GDPR, U.S. companies providing data processing services (including cloud computing services) are also likely to be affected, particularly given that information regarding an individual's location data and online identifier (e.g., IP address) now explicitly constitutes "personal data."

SUMMARY OF EXTRA-TERRITORIAL SCOPE



APPOINTMENT OF A REPRESENTATIVE

Summary

Organisations to which the GDPR apply, but which have no physical presence in the EU, will have to appoint a local representative against whom enforcement action may be taken.

Exceptions apply where the processing (1) is occasional, (2) does not involve large scale processing of sensitive personal data or personal data relating to criminal convictions and offences, and (3) is unlikely to result in a risk to the rights and freedoms of natural persons.

Changes to the Directive

There are no equivalent provisions under the Directive.

Practical Implications

A company that has no EU presence but targets consumers within the EU must carefully consider whether this provision will apply to their operations. The name and contact details of the data controller (or its representative where it is based outside the EU) will need to be included in privacy notices.

If subject to these requirements, your business must give serious consideration to this appointment, especially given the significant liability that a representative must bear (see **Fines**).

APPOINTMENT OF A DATA PROTECTION OFFICER

Summary

A Data Protection Officer (DPO) should be appointed in the following circumstances relevant to U.S. data controllers or data processors – essentially where their core activities:

- Require regular and systemic monitoring of data subjects on a large scale or
- Involve processing sensitive personal data or personal data relating to criminal convictions and offences

Other controllers or processors may still decide to appoint a DPO voluntarily. EU regulators encourage organisations to designate a DPO on a voluntary basis even where the GDPR does not specifically require such an appointment. Given the uncertainty and ambiguity as to whether the appointment of a DPO is required, many companies prefer to take a more cautious approach. Guidance from the European regulators (the Article 29 Working Party) published in November 2016, takes an expansive approach, which any U.S. business should consider. In any case, under the **Accountability Principle**, a controller must be able to demonstrate compliance with the general principles relating to the processing of personal data, including the duty to maintain records of processing activities (which applies to any organization with more than 250 employees).

There is also a new requirement to provide the contact details of the relevant DPO, both to the data subjects (see **Information Requirements**) and to the national supervisory authority.

Changes to the Directive

There was no obligation to appoint a DPO under the Directive, although some Member States — Germany, for example — required the appointment of DPOs and some businesses currently choose to appoint a DPO.

Practical Implications

Where required, a DPO should be appointed who has the necessary professional experience, including expert knowledge of data protection law. The DPO need not work solely for an organisation: a group of undertakings may appoint a single DPO, provided the DPO is easily accessible for all. Further, the DPO need not necessarily be a new or dedicated role within an organisation. The role of the DPO may be allocated to an existing employee provided that his or her duties are compatible with those of the DPO and do not lead to a conflict of interests. DPOs have protected employment status in that they cannot be dismissed or penalised for performing their role (although this should not prevent dismissal for reasons unrelated to their role, e.g., misconduct).

It is also possible to contract out the role of the DPO to a third party, which is helpful given that the resource pool with relevant experience is relatively limited and the processing operations of an individual business may not justify a full-time internal appointment.

INFORMATION REQUIREMENTS AND PRIVACY NOTICES

Summary

The GDPR prescribes, in detail, the information which must be included in a privacy policy. This must be in clear and plain language and be transparent and accessible. The privacy policy must include the following, many (but not all) of which are typically included in privacy policies:

- The identity of the controller (or representative) and, where applicable, the DPO
- The intended purposes of the processing and its legal basis, including details of "legitimate interests" (where applicable)
- (Where the personal data are not obtained via the data subject) the categories of personal data held
- The recipients or categories of recipients to whom personal data will be disclosed
- Any intention to transfer to a third country or international organisation including details of safeguards relied upon
- The data retention period or how that period is determined
- The existence of the rights to access, request erasure, object to processing, data portability (see below) and withdraw consent
- The existence of automated decision-making, including **Profiling** (see below), the logic involved and potential consequences for the individuals involved
- (Where the personal data are obtained via the data subject) details about whether an individual's provision of personal data is a statutory or contractual requirement and whether such provision is mandatory and the consequences of any failure to provide the personal data
- (Where the personal data are not obtained via the data subject) the source of the personal data and, if applicable, whether it came from a public source
- The right to lodge a complaint with the national data protection authority

The privacy notice should be communicated at the time the data are obtained where it comes from the data subject.

Changes to the Directive

While the GDPR requires privacy notices to be concise, easily accessible and easy to understand, it also requires much more detail than what is required under the Directive.

Practical Implications

More information will need to be disclosed, meaning that some privacy policies are likely to need to be reworked. In practical terms, the requirements for transparency and accessibility refer to policies which are easy to find (i.e., on an obvious place on an organisation's website) and in plain, easily comprehensible language (which is often more of a practical challenge). Privacy notices will need to be more specific and granular. Bundled consents covering a number of different uses of personal data will not be sufficient. Businesses will need to review their retention policies in order to be able to specify how long the personal data is retained or the methodology for determining this.

One advantage of the GDPR is that a single notice is likely to be sufficient in all Member States (although it will need to be translated into a local language in order to be deemed "accessible"). Businesses which operate in more than one European country currently need to allow for variances in formal requirements and regulatory practice in each jurisdiction. Although the scope of these variances will be reduced by the GDPR, some will remain and taking account of the nuances may be time consuming and expensive. Regulators are expected to issue guidance on the form and content of privacy notices, which we will summarize as soon as they are issued.

RECORDS OF PROCESSING ACTIVITIES

Summary

Businesses with more than 250 employees must maintain internal records of processing activities. If a business has fewer than 250 employees it must maintain records of higher risk processing activities, such as processing of special categories of data or criminal convictions and offences. Data controllers must maintain:

1. The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer
2. The purposes of the processing
3. A description of the categories of data subjects and of the categories of personal data
4. The categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations
5. Details of transfers of personal data to third countries, including documentation of the transfer mechanism safeguards in place
6. The envisaged time limits for erasure of the different categories of data
7. A general description of the technical and organisational security measures applied to the data

Data processors must maintain:

1. The name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, the representative and data protection officer
2. The categories of processing carried out on behalf of each controller
3. Details of transfers of personal data to third countries
4. A general description of the technical and organisational security measures applied to the data

Changes to the Directive

These requirements replace the obligation to notify data processing activities to local supervisory authorities, which currently apply and vary significantly between Member States. For example, the U.K. only requires relatively brief high-level details of the purposes of processing and types of data being processed, while others (France, for example) require much more detailed information to be filed.

Practical Implications

Businesses will need to keep more detailed records of processing activities and will require an internal audit of processing activities carried out by a business and internal resources to maintain and update the records. Processors who provide services to others are likely to receive requests for such information from customers, and internal record keeping by any business is likely to become a key compliance issue. Warranties addressing these risks are likely to become much more common in service agreements and in M&A transactions.

REQUIREMENTS FOR CONSENT

Summary

The data controller must be able to demonstrate that the requisite consent to processing has been obtained from the data subject, unless it relies on one of the alternative grounds (such as contractual necessity or legitimate interest). Consent is defined as a "freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data." Any request for consent must be in clear and plain language and easily distinguishable from other matters. Importantly, such consent can be withdrawn at any time.

Consent should be given by a "clear affirmative act." It can be given through a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services, or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. However, silence, pre-ticked boxes or inactivity on the part of the user will not constitute consent.

Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for each of those purposes.

If sensitive personal data is being processed, explicit consent is required. This applies to the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data (for the purpose of uniquely identifying a natural person), or data concerning health or a natural person's sex life or sexual orientation.

If data relating to children (under the ages of 13-16, depending on the Member State) are involved, parental consent will be required.

Changes to the Directive

The Directive distinguished between ordinary and "explicit" consent. Whilst the GDPR's basic standard of "consent" is not quite as high as "explicit" consent, nevertheless the standard is very high since an "unambiguous indication" and "clear affirmative act" indicating the data subject's wishes is required. The actual practical difference between "explicit" consent and an "unambiguous indication" of consent is unclear. As noted above, processing of sensitive personal data will always require explicit consent.

Practical Implications

It will be much more difficult to obtain valid consent under the GDPR than under the Directive. However, consent is only one of a number of legal bases for processing an individual's personal data. If the basis of consent cannot be satisfied, another basis, such as the data controller's legitimate interests, could be relied on, although the privacy notice will need to include details of those legitimate interests.

Consent must be specific for the purposes that the data is intended to be used for and it must be shown to be unambiguous agreement (for example, ticking a blank box). Consent must not be part of a standard set of contractual terms. It must be as easy to withdraw consent as it is to give consent.

Businesses will therefore need to ensure that their systems and processes can maintain an audit trail of consents and allow processing to be stopped when consent is withdrawn.

The Article 29 Working Party is due to issue further guidance on the requirements for consent.

LEGITIMATE INTEREST

Summary

This is one of the legal bases for the lawful processing of personal data. In order for a data controller to rely on its (or a third party's) legitimate interests, the interests or the fundamental rights and freedoms of the data subject must not be overriding, taking into account their reasonable expectations.

Examples given in the GDPR include the purposes of preventing fraud, direct marketing and transferring data within a group of companies for internal administrative purposes. However, this does not apply to a transfer outside of the EEA for processing (see further **International Transfers** below).

Changes to the Directive

"Legitimate interests" also currently constitutes a basis for lawful processing under the Directive. However, owing to the difficulties in complying with the requirements for consent as a legal basis for processing under the GDPR, companies are likely to increasingly justify processing based on their legitimate interests.

Practical Implications

Companies should start auditing their use of personal data. The reasons for the collection and use of personal data should be analysed, together with the legal justification(s) to be relied on.

If the legal basis is "legitimate interests," this will need to be communicated to data subjects through privacy notices (see **Information Requirements**). Furthermore, any legitimate interest must not be overridden by the fundamental rights of data subjects. This may be the case if processing for a particular purpose would not reasonably be expected to occur at the time (and in the context that) data is collected. Given the increased penalties for non-compliance, justifying a legitimate interest will require much more detailed supporting analysis.

NEW AND ENHANCED RIGHTS 1: RIGHT TO OBJECT

Summary

The GDPR contains a number of new and enhanced rights for individuals, which may require changes to technology platforms or internal processes.

A data subject has the right to object to the processing of their personal data where the processing is:

- For direct marketing (including profiling)
- Based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- For purposes of scientific/historical research and statistics

A data controller must stop processing personal data for direct marketing purposes as soon as an objection is received. This is an absolute right and there are no exemptions or grounds to refuse. If a business processes personal data based on its legitimate interests or for the performance of a legal task, it must stop processing the personal data unless it can demonstrate that it has compelling legitimate grounds which override the interests, rights and freedoms of the individual concerned or that the processing is for the establishment, exercise or defence of legal claims.

Where an individual can establish grounds which relate specifically to the individual's personal situation, a data controller may be required to stop processing data for research purposes.

Changes to the Directive

While right to object is available under the Directive, the GDPR makes it easier for the individual to exercise the right.

Practical Implications

A data controller must inform individuals of their right to object at the point of first communication, including a privacy notice. This should be presented prominently and separately from other information. Processes should be put in place to acknowledge such rights.

NEW AND ENHANCED RIGHTS 2: AUTOMATED DECISIONS AND PROFILING

Summary

Individuals have the right not to be subjected to decisions based solely on automated processing, including profiling. This provision increases protection and control of profiling and replaces the current provisions on automated decision-making in the Directive.

Profiling is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects," in particular performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement. Examples include automatic credit assessment or e-recruiting which do not involve any element of human intervention. The right does not apply where the decision is based on the explicit consent of an individual or is necessary for a contract with the individual – subject to the data controller implementing suitable measures to safeguard the data subject's rights – including the right to contest the decision and obtain human intervention in the decision-making process.

Changes to the Directive

The GDPR gives greater prominence to this right and makes it easier for data subjects to opt out of being profiled.

Practical Implications

Depending on the purpose of the profiling, companies may fall outside the scope of this provision. For example, profiling for marketing purposes (provided that it is not performed on a scale that may restrict an individual's access to goods and services) is unlikely to have any legal effect (or other similarly significant effect) on an individual.

Generally, profiling will require the consent of the individual and, if profiling is based on sensitive personal data, consent must be explicit.

When companies engage in profiling, they must ensure that the processing is fair and transparent by providing meaningful information about the logic involved. They must also implement appropriate statistical procedures to minimise errors and correct inaccuracies and, where appropriate, include a right for human review and intervention.

The Article 29 Working Party is due to issue further guidance on profiling.

NEW AND ENHANCED RIGHTS 3: RIGHT TO DATA PORTABILITY

Summary

A data subject has, in certain circumstances, the right to obtain from the data controller, on request, a copy of all personal data that the controller processes, which the data subject provided. The data controller must provide the data in a commonly used electronic and structured format (e.g., Excel) that permits further use by the data subject. Supporting explanatory materials must also be provided if relevant.

This only applies where the processing is carried out by automated means and the personal data was obtained on the basis of consent, or was necessary for the performance of a contract. It is not available where the personal data have been obtained on other grounds (e.g., compliance with a legal obligation).

This provision will be primarily relevant for online services and aims to enable data subjects to move their data between online providers without losing previously disclosed data or having to input it again.

Changes to the Directive

This is a new right that did not exist in the Directive.

Practical Implications

The data must be provided free of charge (although a reasonable fee may be charged for further copies). Requests may be refused if the data controller can prove that they are unfounded or excessive. Any request must be complied with within one month (with extensions in some cases) and any intention not to comply must be explained to the individual.

It would be advisable to consider whether data held by a business can be easily exported (especially in machine-readable and inter-operable formats). Instances where the data relates to more than one individual, but is requested by one individual, may raise confidentiality implications. The GDPR provides that the right must "not adversely affect the rights and freedoms of others", and Member States are likely to have additional laws governing this.

NEW AND ENHANCED RIGHTS 4: RIGHT TO ERASURE (RIGHT TO BE "FORGOTTEN")

Summary

Individuals may request the deletion of their personal data where:

- Data are no longer necessary for the purpose for which it was collected or processed
- The individual withdraws consent (and there are no other legal grounds for processing)
- There are no overriding legitimate grounds for the processing which the controller is able to demonstrate
- The data are otherwise unlawfully processed (i.e., in breach of the GDPR)
- The data have to be erased to comply with EU/ Member State law (i.e., legislation stipulating that such data may only be held for a specified period of time)

The GDPR provides exemptions where processing is necessary:

- For the exercise of the right of freedom of expression and information
- For compliance with legal obligations

- For performance of a public interest task/exercise of official authority
- For public health purposes in the public interest
- For archival, research or statistical purposes
- For the exercise or defence of legal claims

Changes to the Directive

This provision expands the rights of data subjects. There is a similar provision in the Directive, although erasure is limited to processing that causes unwarranted and substantial damage or distress.

Practical Implications

Compliance will potentially be very onerous and it is unclear at present, given the exemptions available and the conflict of fundamental rights that may result, how this will be implemented in practice. A fact-based analysis should be undertaken on a request by request basis.

NEW AND ENHANCED RIGHTS 5: RIGHT TO RESTRICT PROCESSING

Summary

The right to erasure needs to be considered in the context of the right for a data subject to require a data controller to restrict processing where:

- The accuracy of the personal data is contested by the data subject (in which case, processing should be restricted until the accuracy has been verified)
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims
- The data subject has objected to processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the data controller is deciding whether its legitimate grounds for processing override the rights of the data subject

Changes to the Directive

This provision clarifies and expands the existing principles.

Practical Implications

Businesses should ensure that their systems allow data to be segregated to limit access to the data, so that it can be stored, but not subjected to any further processing.

DATA PROTECTION BY DESIGN AND DEFAULT

Summary

Data controllers must ensure that new technologies and business models are designed in a way which limits the processing of personal data to what is necessary to achieve the purpose for which it was collected. Access to personal data should be limited to those who need it within the organisation.

Data protection "by design" involves taking appropriate technical and organisational measures to implement data protection principles (e.g., the use of pseudonymisation techniques so that personal data cannot be attributed to a specific individual without additional, and separately kept, information or identifiers) when creating new products and services or engaging in other processing activities. Data protection "by default" includes the principle of data minimisation, which applies to the amount of personal data collected and the extent to which it is processed, retained and is capable of being accessed. It should be noted that the GDPR does not apply to anonymous information or its processing (including for statistical or research purposes). This includes information which does not relate to an identifiable individual and personal data rendered anonymous so that the data subject is no longer identifiable. Many vendors (ranging from providers of basic HR services through to complex data analytics) retain the right to use anonymized data taken from a particular customer for the purposes of aggregation in to a wider dataset for the benefits of their customers as a whole. Customers will need to ensure that they comply with appropriate technical standards relating to anonymization.

Changes to the Directive

Privacy by design and privacy impact assessments have long been recommended by regulators as a matter of good practice, but have not previously been formal legal obligation. Regulators will have increased scope to look at businesses' internal processes and procedures to ensure that key principles are observed.

Practical Implications

Businesses must now consider data protection implications from the inception of any new technology, product or service that involves data processing.

Privacy impact assessments (see **Technological and Organisational Changes**) will also be required to identify privacy risks in new products. Any measures must be implemented to integrate the necessary safeguards. However, the GDPR allows for a risk-based approach given the cost of implementation and the nature of the processing in question. In essence, new products and processes should be designed from inception with data privacy in mind.

TECHNOLOGICAL AND ORGANISATIONAL CHANGES

Summary

Businesses will be required to carry out an assessment of the impact of planned processing arrangements, particularly where new technologies are used and the processing is likely to result in a high risk to the rights and freedoms of individuals. Many companies already do this as part of the development of a new product or service, although it is something that is often overlooked. PIAs will be required where, broadly, there is (1) systematic and extensive evaluation which is based on automated processing, including profiling; (2) the processing is on a large scale of sensitive personal data; or (3) there is systematic monitoring of a publicly accessible area on a large scale.

Controllers must consult with the relevant supervisory authority when a PIA suggests that there would be a high risk to individuals in the absence of measures taken to mitigate that risk. However, it is unclear whether this must be done in all circumstances or only where the risk cannot be mitigated by reasonable means.

Changes to the Directive

PIAs were not legally required under the Directive, but are now mandatory in the circumstances stipulated. PIAs are a key part of adopting a "privacy by design" approach.

Practical Implications

PIAs must, as a minimum, provide:

- A description of the processing operations, their purpose and, where applicable, the legitimate interest pursued
- An assessment of the necessity and proportionality of the processing operations in relation to their purposes
- An assessment of the risks to the rights and freedoms of data subjects
- The measures envisaged to address the risks

Technical teams will need to involve legal and risk professionals much earlier in the product design and development process to avoid potentially expensive re-engineering of systems and processes. Consultation with a supervisory authority is likely to take some time, which should be factored in to the development timetable.

Further guidance is expected from regulators on the specific types of processing activity for which PIAs will be required.

DATA SECURITY AND BREACH NOTIFICATION

Summary

The GDPR introduces, for the first time, pan-European data breach notification rules. The basic concept and many of the principles will be familiar to U.S. businesses which need to comply with federal statutes in specific sectors (notably the Health Insurance Portability and Accountability Act in the health care sector and the Gramm–Leach–Bliley Act in the financial services sector) and 48 state laws.

Previously, data breach notifications were mandatory only in some EU countries (e.g., Germany and Austria). A personal data breach is 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.

A controller must notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it (unless such breach is unlikely to result in a risk to the rights and freedoms of natural persons). A notification after 72 hours should be accompanied by an explanation for the delay. Data processors must inform controllers of any data breach they become aware of without undue delay.

Data subjects must be informed without undue delay where the breach is likely to result in a high risk to their rights and freedoms, unless the data has been rendered unintelligible to any third party (e.g., by encryption). The data subject should be told about the nature of the breach, the contact details of the DPO (or other point of contact) and any measures to mitigate the effects of the breach.

Changes to the Directive

There is currently no general obligation for businesses to notify a breach to DPAs or data subjects. However, regulators in some EU countries, such as the U.K., Denmark and Ireland, have issued guidelines advising businesses to voluntarily report any serious breach, and other Member States have implemented breach reporting obligations in national law (Germany and Austria, for example).

Practical Implications

Many U.S. states have tightened notification timelines, moving from "the most expedient time possible" down to 14 days for preliminary notices in Vermont. However, a 72 hour timeframe is extremely ambitious and generally only allows time for preliminary steps to identify and investigate the breach, with full containment taking an average of around 70 days.

Data controllers must compile an internal breach register, which it must keep regardless of whether the breach requires notification. This should include details of the facts relating to a breach, its effects and remedial action taken. Companies should draft or reassess their data breach response procedures accordingly and work with their IT teams to implement, and keep under review, appropriate technical and organisational measures to safeguard against disclosure. Businesses should consider the adoption of a cybersecurity framework (such as ISO 27001-2), draft robust incident response plans, and carry out regular tests and internal training. Customers will need to review contractual disclosure requirements in agreements with their vendors, and should also review insurance policies to assess the extent of coverage.

The Article 29 Working Party is due to issue further guidance on data breach notification.

VENDOR MANAGEMENT

Summary

The GDPR more closely scrutinises the relationship between controllers and processors. Controllers make the decisions about processing, whether or not they carry out the actual processing themselves. Controllers must not use processors that do not provide sufficient guarantees to implement appropriate data protection safeguards and comply with the GDPR.

Changes to the Directive

The Directive was largely focused on the activities of data controllers, and data processors were subject to much lighter obligations (although over ten Member States opted to regulate controllers directly under national laws). The GDPR applies directly to processors, and processors are subject to fines or other penalties (which were previously generally restricted to data controllers).

The Directive currently places relatively light mandatory obligations for controllers to include in contracts with processors: a written agreement, stipulating that the processor should only act on the controller's instructions and should implement appropriate technical and organizational measures to protect personal data. In addition, the GDPR requires that processors must:

- not appoint sub-processors without specific or general authorization of the controller and to ensure there is a contract with the sub-processor containing minimum terms
- only process personal data on the instructions of the controller unless required to process for other purposes by EU or Member State Law – this does not include a foreign law such as US law, raising potential conflicts for US processors
- appoint a representative if based outside of the Union
- keep a record of all categories of processing activities carried out on behalf of a controller
- cooperate on request with supervisory authorities
- notify the controller without undue delay as soon as it is aware of any personal data breach
- appoint a data protection officer where required
- comply with the rules on transfers of personal data outside of the EU

Practical Implications

Controllers should assess whether the processors they engage have sufficient capabilities to meet all the requirements of the GDPR. This may involve vetting existing and/or prospective processors.

Controllers should audit their existing activities in relation to processing and ensure that all processors are engaged on legal contracts satisfying the minimum provisions.

SANCTIONS

Summary

Fines for non-compliance are potentially vast — up to 4 percent of the total worldwide annual turnover or €20,000,000 (whichever is higher). This range of fines applies to many of the core provisions of the GDPR, including the six general principles of processing. There is also a lower tier of fines — up to €10,000,000 or 2 percent of total worldwide annual turnover (whichever is higher). This applies to certain failures, such as failure to appoint a Data Protection Officer; implement appropriate technical and organisational security measures; maintain written records; or report a data breach. These levels do not necessarily bear any relation to the actual harm caused to a data subject, and are largely symbolic and intended to raise data protection compliance issues to the highest board level.

In addition, national supervisory authorities will have extensive investigative powers, including powers to carry out investigations and audits, require corrective measures to be taken, impose temporary or permanent bans on processing, or suspend international transfers of data.

Changes to the Directive

Currently, fines vary under national laws and are relatively low (for example the statutory maximum fine in the U.K. is £500,000). Under the GDPR, the amount that can be fined on breach has been substantially raised and harmonised across the EU, and the range of powers open to supervisory authorities has expanded significantly.

Practical Implications

The legal and financial risk to businesses of data protection breaches has increased substantially. Companies should re-evaluate their compliance priorities correspondingly. While the headline numbers for potential fines are vast, regulators will take into account a wide range of factors when determining fines, including:

1. The nature, gravity and duration of the infringement
2. Whether infringement was intentional
3. Categories of personal data affected
4. Steps to mitigate the damage suffered
5. Degree of responsibility (e.g., data protection by design or by default) or any relevant previous infringements
6. Adherence to a code of conduct (or certification mechanism)
7. Cooperation with the supervisory authority (and the manner in which supervisory authority learned of infringement)
8. Compliance with measures ordered
9. Other aggravating or mitigating factors (e.g., financial benefits, etc.)

INTERNATIONAL DATA TRANSFERS

Summary

Personal data may only be transferred to third countries outside of the European Economic Area which are deemed by the European Commission to offer an adequate level of protection (the United States is not one of those few countries) or where adequate safeguards are in place in respect of the processing in those third countries, including:

- Use of standard contractual clauses mandated by the European Commission
- Binding corporate rules (agreements governing transfers made between members of a corporate group and approved by national regulators)
- An approved certification mechanism as provided in the GDPR

The GDPR permits derogations in certain circumstances. One of these derogations is the explicit consent of the data subject after having been informed of all the risks. Given the high standard required for "explicit" consent, this will only apply in limited situations.

Changes to the Directive

This is an area where there are relatively few changes, which in some ways is welcome after a turbulent period following the demise of the EU-U.S. Safe Harbor Scheme in 2015. Binding Corporate Rules were developed from guidance by European data protection authorities and are now formally recognized under the GDPR. The GDPR provides for a "minor transfer exemption" that permits transfers of limited amounts of personal data to third countries in the absence of an adequacy decision or other permitted justification. However, the scope of this exemption is very narrow and it is unlikely to be of much practical value to controllers.

Practical Implications

U.S. companies can continue to rely on existing mechanisms for data transfers — principally standard contractual clauses or certification under the EU-U.S. Privacy Shield. The key practical point for companies is that contravention of the data transfer rules can lead to fines in the highest range of up to €20,000,000 or 4 percent of worldwide revenue. They could also result in supervisory authorities exercising their powers to suspend data flows to third countries. Implementing appropriate safeguards is therefore a critical issue which cannot be viewed as a minor compliance issue.

KEY CONTACTS

Huw Beverley-Smith
Partner, London
T: +44 (0) 20 7450 4551
huw.beverley-smith@FaegreBD.com

Jonathon Gunn
Trainee Solicitor, London
T: +44 (0) 20 7450 4512
jonathon.gunn@FaegreBD.com

Paul Luehr
Partner, Minneapolis
T: +1 612 766 7195
paul.luehr@FaegreBD.com

Midori Okamoto
Associate, London
T: +44 (0) 20 7450 4569
midori.okamoto@FaegreBD.com

Kathleen Rice
Counsel, South Bend
T: +1 574 239 1958
kathleen.rice@FaegreBD.com

Leita Walker
Partner, Minneapolis
T: +1 612 766 8347
leita.walker@FaegreBD.com

FAEGRE BAKER DANIELS

FaegreBD.com

UK ▾ USA ▾ CHINA