FAEGRE BAKER DANIELS

The EU General Data Protection Regulation: Practical Implications for Businesses

TABLE OF CONTENTS

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 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 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 about data privacy, mean that compliance with data privacy laws cannot be treated as a minor regulatory issue. Potential fines and other penalties under the GDPR will put data privacy and cybersecurity at the same level as antitrust or anti-bribery and corruption programs 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 legal representatives who will accept liability for rule violations
- 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 within the EU around data privacy and security issues although some national 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 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 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 company will potentially be covered, even if it does not have a business presence in the EU, and only markets to EU based consumers or monitors their behaviour.

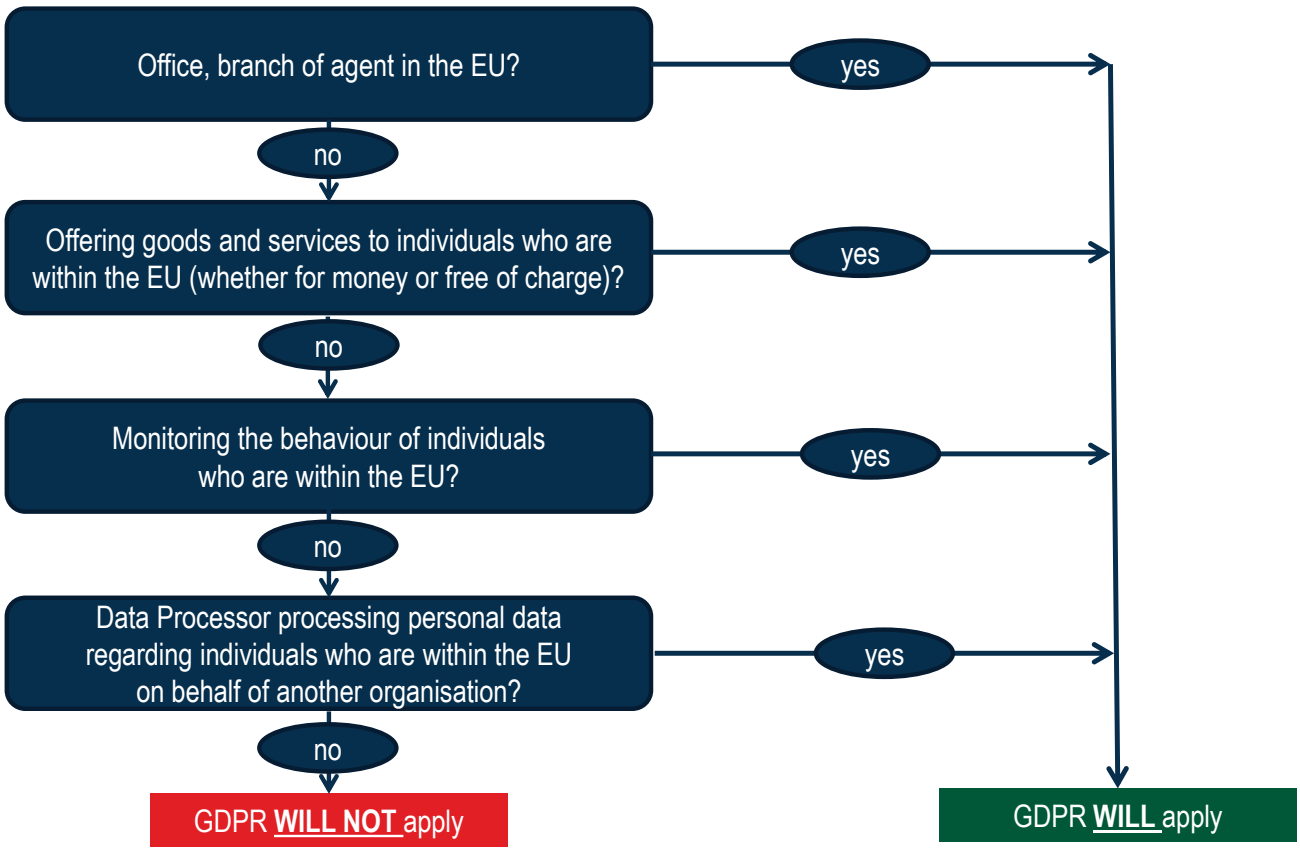
Furthermore, whereas the Data Protection Directive mainly covered the activities of a data controller (i.e., the business which decides on the purposes and means by which the processing is carried out), the GDPR will also directly cover data processors (i.e., those companies that handle data on behalf of another business or customer).

Practical Implications

The widened scope means a vast range of 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 outside the EU will be caught if they collect and handle data of EU customers in the course of offering goods or services. 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. Also, data processors can be sued directly by regulators and consumers under the GDPR without having to go through the data controller. This puts cloud computing and other hosting or management services at greater risk, particularly given that information regarding an individual's location data and online identifier (e.g., IP address) will explicitly constitute "personal data."

SUMMARY OF EXTRA-TERRITORIAL SCOPE



APPOINTMENT OF A REPRESENTATIVE

Summary

Organisations to which the GDPR applies, 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 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 and EU regulators encourage organisations to do so. 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 to this requirement. In practical terms, a person like a DPO will likely be needed in any case under the GDPR's **Accountability Principle** because any business that is a controller with more than 250 employees must be able to demonstrate compliance with the general principles related to processing personal data, including the duty to maintain records of such activities.

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 one organisation: a group of legal entities 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 interest. DPOs have protected employment status and 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 talent pool for such people 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 to consumers. The privacy policy must include the following:

- 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)
- The categories of personal data held, if the data subject did not provide the information directly
- 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 right to access, request erasure, object to processing, move data (see "Data Portability" 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 will require privacy notices to be concise, easily accessible and easy to understand, it also will require much more detail than the Directive.

Practical Implications

More information will need to be disclosed, meaning that many privacy policies will 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 also 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 different local languages 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 it is 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 those related to children, health care information, 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 to erase 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(s) and 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 will replace the obligation to notify data processing activities to local officials, which vary significantly between Member States. For example, the U.K. only requires relatively brief high-level information about the purposes of processing and types of data being processed, while other countries like France 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 and internal resources to maintain and update records. Processors who provide services to others are likely to receive detailed requests for information from customers so internal recordkeeping 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

To collect and handle the personal information of individuals in the EU, some businesses will be able to point to their contract terms or some "legitimate interest" (e.g. fraud prevention); however, many other businesses will need to demonstrate they have received proper consent from EU consumers or employees. 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 on an ISP or social media site or another statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of his or her personal data. However, silence, pre-ticked boxes or user inactivity 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 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 (see Children and Consent).

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, although the UK Information Commissioner has suggested that "explicit" consent will require express confirmation in words. 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 (see below), could be relied on, although the privacy notice will need to include details of those legitimate interests.

Consent must be specific to the intended purpose and use of the data collected and must be unambiguous (e.g. demonstrated by ticking a blank box). Consent cannot be presumed from 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.

CHILDREN AND CONSENT

Summary

The importance of protecting children's personal data is mentioned frequently in the GDPR. In recognizing children as "vulnerable individuals", the GDPR makes express provisions for consent provided by children in Article 8.

The GDPR requires parental consent to be obtained before processing a child's personal data when "information society services" are being offered. "Information society services" include most internet services normally provided for remuneration, and protection is especially significant where the personal information is to be used to create online profiles, or for marketing.

The requirement for parental consent applies to the processing of personal data of children aged under 16, although the GDPR allows for this age threshold to be lowered by member state law, with a lower limit of 13.

The data controller is also required to make "reasonable efforts" to verify, through available technology, that consent has been provided by the holder of parental responsibility. The GDPR envisages the creation of codes of conduct to assist businesses in navigating this requirement.

Importantly, the requirement for parental consent is applicable only where the processing would be based on the child's consent. It is unclear whether this requirement would extend to apply in situations in which children's personal data is unintentionally collected online.

Parental consent is not required in the context of preventative or counselling services offered directly to a child.

Changes to the Directive

The Directive did not impose explicit or specific restrictions on the processing of children's personal data, and such processing was subject to national laws. Article 8 of the GDPR is a significant change in this regard, although it does not specifically prescribe the age at which a person is no longer considered a child.

The GDPR also introduces the principle of transparency and requires that information addressed to the public or data subject is easily accessible and understandable through the use of plain language and, where appropriate, visualization (see Information Requirements and Privacy Notices). As such, any information and communication surrounding processing aimed at a child will need to be in clear and easily understandable language.

Practical Implications

The variable age threshold in the context of parental consent is likely to cause difficulties for companies operating internationally or across a number of EU member states. It is expected that many member states will opt for the lower age of consent of 13.

As the GDPR does not define when an individual is no longer a child, controllers will have to ensure any information or communication addressed to children is suitable for the relevant age range, and will need to implement these requirements into notices aimed at both teenagers and young adults.

However, the remit of Article 8 extends only to certain online data, and offline data will continue to be governed in line with individual member state rules. Similarly, Article 8(1) does not affect general contract law in member states with regards to the validity, formation or effect of a contract with a child. National legislation will need to be heeded when dealing with such contracts.

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 European Economic Area (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, it will be much more difficult to demonstrate consent under the GDPR; therefore, 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 their legal justifications.

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 statistical research

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 other overriding grounds or needs to establish a legal claim.
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 the 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, for example by a privacy notice on a website. This should be presented prominently and separately from other information. Businesses also must establish more sophisticated ways to track objections and stop processing for specific people.

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 protections against 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 a business profiles an individual based on the explicit consent of that individual or when necessary to contract with the individual – subject to the adoption of measures to safeguard the data subject's rights, including the right to contest a 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 profiling, many companies may fall outside the scope of this provision. For example, if a business profiles for marketing purposes but does not restrict an individual's access to goods and services, the profiling may not have any legal effect on the individual.

Generally, if profiling does have a legal or similarly significant effect on an individual (e.g. limiting a person's access to a loan), it 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, and must provide meaningful information about the logic involved. They must also implement appropriate statistical procedures to minimise errors and correct inaccuracies. Where appropriate, companies must 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

In certain circumstances, a data subject will have the right to request the data controller to provide a copy of all processed personal information originally provided by that person. The data controller will need to provide the data in an electronic and commonly used structured format (e.g., Excel) that permits further use by the data subject. Supporting explanatory materials will need to be provided if relevant.

This provision will only apply 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. The provision will not apply to other types of processing (e.g., compliance with a legal obligation).

This provision will mainly cover online services and aims to enable individuals to move their data between online providers without losing 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

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

Online companies should consider whether data about specific customers can be easily exported (especially in machine-readable and inter-operable formats). Confidentiality may be a concern where combined data relates to more than one individual. The GDPR does state that data requested 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 will have the right to request the deletion of their personal data where:

- Data are no longer necessary for their original, stated purpose
- The individual withdraws consent (and there are no other legal grounds for processing)
- The controller cannot demonstrate overriding legitimate grounds for additional processing
- 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 currently limited to processing that causes unwarranted and substantial damage or distress.

Practical Implications

This provision could place very onerous requirements on companies. Given the exemptions available and the potential conflict with other fundamental rights (e.g., rights to free speech and the press) it is unclear how this provision will be implemented in practice. Companies should carefully analyze the facts of each specific, erasure request.

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 for the 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 can segregate and store personal data so that access can be limited without 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

protect personal information when creating new products and services or engaging in other processing activities. This may require, for example, using pseudonymisation techniques so that personal data cannot be attributed to a specific individual without additional information or identifiers that are kept separate). Data protection "by default" includes the principle of data minimization that should limit the amount of personal data collected, processed, accessed or retained. It should be noted that the GDPR does not apply to anonymous information or personal data that cannot be traced back to identifiable individuals. Many vendors, like data analytics companies or HR services, claim to use anonymized data taken from particular users and employees and aggregate it for the benefit of their customers as a whole. Businesses that allow this activity or perform such analysis 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 a formal legal obligation. Regulators will have increased scope to look at businesses' internal processes and procedures to ensure that these key principles are observed.

Practical Implications

With the inception of any new technology, product or service that involves personal data, businesses will need to implement procedures to protect that data.

Privacy impact assessments (see **Technological and Organisational Changes**) will also be required to identify privacy risks in new products. However, the GDPR allows for a risk-based approach based on 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 assess the impact of planned processing arrangements, particularly those involving new technology and a high risk to the rights and freedoms of individuals. Fortunately, many companies around the world already do this when they develop a new product or service. Under the GDPR, PIAs will generally be required where there is (1) profiling or other types of systematic and extensive evaluation based on automated processing (2) large scale processing of sensitive personal data; or (3) 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 many circumstances. 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 expensive re-engineering of systems and processes. Companies will also need to factor in the time required to consult with their supervisory authorities should any issue arise.

Further guidance is expected about 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. Previously, data breach notifications were mandatory only in some EU countries (e.g., Germany and Austria). Now they will be required by companies doing business across the EU. 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 within 72 hours of becoming aware of it. A notification after 72 hours will need to be accompanied by an explanation for the delay. Data processors must inform controllers of any data breach without undue delay.

Individual 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 was rendered unintelligible to any third party (e.g., by encryption). Companies need to tell data subjects about the nature of the breach, the contact details of their DPO (or other point of contact) and any steps taken to mitigate the effects of the breach.

Changes to the Directive

There is currently no general obligation for businesses to report 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 serious breaches, and other Member States have required breach reporting under national law (Germany and Austria, for example).

Practical Implications

The new EU 72 hour timeframe will set the bar high. This deadline will generally only allow time to copy down important data and begin the investigation. Surveys show that a full investigation and containment typically takes about 70 days; therefore, early notices to regulators will be perfunctory and justifications for “delay” past 72 hours will be common.

Data controllers must compile an internal breach register, regardless of whether a breach triggers notification. The register should include detailed facts about each incident, its effects and remedial action taken. Companies should draft or reassess their data breach response procedures accordingly and work with their IT teams to review and implement appropriate technical and organisational safeguards. Businesses should consider adopting a cybersecurity framework such as ISO 27001-2 and carry out regular tests and internal training. In addition, businesses will need to review their insurance coverage for cyber risks, as well as security and breach notification clauses in their vendor contracts.

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 safeguard data and comply with the GDPR.

Changes to the Directive

The Directive largely focused on the activities of data controllers, whereas data processors in any Member States were subject to much lighter obligations. In contrast, the GDPR will apply directly to processors and subject them to potential fines or other penalties.

The Directive currently places relatively light mandatory obligations on contracts between controllers and processors: a written agreement, stipulation that the processor should only act on the controller's instructions and should implement appropriate technical and organizational measures to protect personal data. The GDPR will impose these conditions as well as many others. Under the GDPR 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 laws, raising potential conflicts for 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 have the ability to meet all the requirements of the GDPR. This may involve more rigorous vetting of existing and/or prospective processors.

Controllers also should audit their existing processing activities and agreements to ensure that all processing is covered by appropriate legal contracts that satisfy the GDPR provisions.

SUPERVISORY AUTHORITIES AND THE CONSISTENCY MECHANISM

Summary

One of the underlying aims of the GDPR is to harmonize data protection laws across the European Union. Whereas the Directive required national legislation to be passed by each EU member state in order to come into effect (which created a patchwork of laws across the EU according to the interpretations of each EU member state) the GDPR will be directly applicable and enforceable in all EU member states.

Under the GDPR, national supervisory authorities, otherwise known as "data protection authorities" (DPAs), are tasked with ensuring the consistent application of the GDPR across the European Union. Their role includes promoting awareness of the risks, rules and safeguards pertaining to personal data as well as advising national and governmental institutions on the application of the GDPR.

The GDPR also introduces the concept of the "one-stop-shop" to provide a single, uniform decision-making process in circumstances in which multiple regulators have responsibility for regulating the same activity performed by the same organisation in different EU member states. In theory, the "one-stop-shop" will mean greater harmonisation, and the more uniform application of EU data protection law, as an organisation will generally deal with a single lead DPA.

Finally, the GDPR establishes the European Data Protection Board (EDPB) to ensure the consistent application of the GDPR on a pan-European level. A key function of the EDPB is to resolve any disputes that arise where DPAs disagree on a particular matter or interpretation. In these instances, the EDPB, as a central authority, can make a binding decision on the matter in issue. The tasks of the EDPB are wide-ranging, including issuing guidelines, recommendations and best practices on GDPR-related matters, encouraging the creation of codes of conduct, and promoting the cooperation and effective multilateral exchange of information between supervisory authorities.

Changes to the Directive

In practical terms, whether an organisation will notice a significant change will depend on whether it operates in one or across multiple EU member states. The roles and responsibilities of national DPAs remain largely unchanged and so the impact on those organisations that operate in only one EU member state will be minimal.

However, the new "consistency mechanism" will assist businesses with operations across multiple member states. Broadly, this applies in two circumstances: (1) where a national DPA intends to take certain action in relation to matters specified in article 64(1) of the GDPR, and (2) where a national DPA requests that a matter of general application or producing effects across multiple EU member states be examined by the EDPB. In such circumstances, the EDPB must produce an opinion on the matter or draft decision within 8 weeks (extended to 14 weeks in complex cases). In exceptional circumstances in order to safeguard the rights of data subjects, a national DPA can implement emergency measures lasting up to three months without going through the consistency mechanism.

In principle, the consistency mechanism will ensure that organisations will encounter consistent compliance requirements across the EU member states in which they do business. However, in practice, there is a risk that the EDPB will face large numbers of requests from concerned DPAs, which may lead to delay and the inconsistent application of the relevant principles. Furthermore, businesses and data subjects have no direct input into the consistency mechanism, which raises concerns regarding the transparency of the process.

Practical Implications

In order to illustrate the application of the regulatory framework, let us imagine that Business A would like to qualify for the one-stop-shop in order to simplify its EU data protection compliance obligations by dealing with, as far as possible, a single, national DPA. Business A is headquartered in New York, and has EU operations in the UK, France, Germany and Spain. Most of its data processing operations take place on a "cloud" platform, rather than at individual locations.

In order to qualify for the one-stop-shop, Business A would need to have a "place of main establishment" in the EU (i.e., a headquarters for its operations in the EU, or a location at which it takes decisions regarding processing activities in the EU). If Business A does not have a place of main establishment in the EU, it will not qualify for the one-stop-shop, and will instead continue to deal with the national DPA in each EU member state in which it operates. It will be up to each business, on a case by case basis, to decide whether it wishes to establish a "place of main establishment" in the EU to benefit from the one-stop-shop mechanism.

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.)

REMEDIES AND LIABILITY

Summary

The GDPR grants a right to compensation to persons who have suffered damage as a direct result of processing operations which infringe the GDPR. This includes material and non-material damage. Both controllers and processors may be liable to the extent that the damage results from the breach of provisions which apply to them (but will not be liable if they are able to prove that they were not in any way responsible for the event giving rise to the damage).

Under the GDPR, every data subject who believes their rights have been infringed can lodge a complaint to a national supervisory authority. Importantly, the GDPR clarifies that a data subject has a number of options in terms of which supervisory authority he or she lodges their complaint – either (a) the supervisory authority in the EU member state in which they reside or work, or (b) the supervisory authority in the EU member state in which the alleged infringement occurred.

The GDPR further clarifies that data subjects may bring judicial proceedings against a controller or processor either in the EU member state in which the controller or processor is established or in the data subject's home member state.

The GDPR extends the scope of liability to processors as well as controllers, which is a notable change from the situation under the Directive. Relatedly, joint controllers (and processors) are fully liable in respect of any compensation payable, with the ability to bring proceedings against the other party for their proportion.

Changes to the Directive

With regards to remedies, there have been relatively few changes as compared with the Directive. Many of the changes involve clarifications and minor extensions of existing law, such as the increased choice given to data subjects in terms of where they lodge any complaint or bring judicial proceedings.

The biggest change in terms of liability is the extension of liability to processors as well as controllers. It is also notable that each party (e.g. controller, joint controller, or processor) will be potentially liable for the full amount of any compensation levied.

Practical Implications

Businesses should be aware that increased data subject choice as regards where they file complaints or launch judicial proceedings may result in businesses having to deal with supervisory authorities and other legal bodies in jurisdictions with which they are unfamiliar. This is particularly the case for

international businesses with operations across a number of EU member states. Whilst the GDPR does harmonize data privacy law considerably, nevertheless certain matters will remain subject to national law and jurisdiction and, to the extent permitted, data subjects can be expected to "shop around" for the most favourable jurisdiction in which to commence any action.

The extension of liability to processors will obviously affect any businesses providing such services. More generally, businesses should expect vendor management and due diligence to become increasingly important and rigorous (see Vendor Management) given that it is possible for organisations to be liable for the other's breach (albeit with the ability to recoup any proportion due).

INTERNATIONAL DATA TRANSFERS

Summary

Personal data may only be transferred to third countries outside of the EEA which are deemed by the European Commission to offer an adequate level of protection 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

Companies can continue to rely on existing mechanisms for data transfers — principally standard contractual clauses or certification, for example, 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.

GDPR GLOSSARY

Accountability – a new principle in the GDPR which requires that a Data Controller be responsible for, and be able to demonstrate compliance with, the data protection principles set out in Article 5(1).

Anonymization – the process of irreversibly preventing the identification of an individual from a set of data.

Biometric Data – any personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of an individual which allows their unique identification, for example, facial images or dactyloscopic data.

Consent – any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she signifies agreement to the processing of personal data by statement or clear affirmative action.

Data Concerning Health – any personal data related to the physical or mental health of an individual which reveals information about his or her health.

Data Controller – the individual or entity that determines the purposes, conditions and means of the processing of personal data.

Data Portability – the right for a data subject to receive the personal data concerning him or her in a structured, commonly-used and machine-readable format and to have such data transmitted to another controller.

Data Processor – the individual or entity that processes personal data on behalf of a Data Controller.

Data Protection Impact Assessment – commonly known as a "privacy impact assessment", a tool used to identify, evaluate and mitigate the privacy risks to individuals of certain processing operations, which is mandated in certain circumstances under the GDPR.

Data Protection Officer – an expert on data privacy who is involved in all issues which relate to data protection and who works independently to ensure that an organization is complying with its obligations under the GDPR.

Data Subject – an individual whose personal data is processed by a Data Controller or Data Processor.

Encrypted Data – personal data protected through technological measures (that convert the data into code) which renders the data accessible only to those with the correct "key".

Enterprise – any individual or entity engaged in economic activity, regardless of legal form, including partnerships and associations.

Filing System – any structured set of personal data that is accessible according to specific criteria.

Genetic Data – any personal data concerning the characteristics of an individual which are inherited or acquired and which give unique information about the health or physiology of the individual.

Main Establishment – in respect of a Data Controller, the place in the European Union that the main decisions regarding the purposes and means of data processing are made; in respect of a Data Processor, the establishment in the European Union where the main processing activities in the context of the activities of an establishment take place.

Personal Data – any information relating to an identified or identifiable natural person (i.e. a Data Subject).

Personal Data Breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Privacy by Default – an approach to projects and systems that ensures that, by default, only personal data which are necessary for each specific purpose of the processing are processed (and a general obligation of a Data Controller under Article 25 of the GDPR).

Privacy by Design – an approach to projects and systems that promotes privacy and data protection compliance from inception (and a general obligation of a Data Controller under Article 25 of the GDPR).

Processing – any operation(s) performed on personal data, whether or not by automated means.

Profiling – any automated processing of personal data intended to evaluate personal aspects relating to an individual, including analysing or predicting a Data Subject's attitudes, interests, characteristics or behaviour.

Pseudonymisation – the processing of personal data such that it can no longer be attributed to a specific Data Subject without the use of additional data, provided that the additional data is kept separately and subject to such measures as to ensure non-attribution to a Data Subject.

Recipient – any individual or entity to which personal data are disclosed.

Representative - any individual or entity established in the European Union explicitly designated by a Data Controller or Data Processor and who represents the Data Controller or Data Processor with regards to their obligations under the GDPR.

Right to Erasure – commonly known as the "right to be forgotten", the right of a Data Subject in certain circumstances to require a Data Controller to erase his or her personal data.

Right to Access – commonly known as a "subject access right", the right of a Data Subject to require a Data Controller to confirm whether it is processing the Data Subject's personal data and, where the Data Controller is processing personal data, to access certain information in respect of this processing.

Supervisory Authority – also known as a "data protection authority" or DPA, a public authority which is established by a European Union member state in accordance with Article 51 of the GDPR and which is tasked with the protection of data and privacy as well as the monitoring and enforcement of the GDPR.

Transparency – a new principle in the GDPR which requires that any information provided to, or communication with, a Data Subject is concise, transparent, intelligible, in an easily accessible form, and uses clear and plain language.

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