McDermott Will & Emery

Special Report

The General Data Protection Regulation: Key Requirements and Compliance Steps for 2018

Authors:

Ashley Winton
+44 20 7577 6939
awinton@mwe.com
London

Romain Perray
+33 1 81 69 15 27
rperray@mwe.com
Paris

Sabine Naugès
+33 1 81 69 15 06
snauges@mwe.com
Paris

Paul McGrath
+44 20 7577 6914
pmcgrath@mwe.com
London

Mark E. Schreiber
+1 617 535 3982
mschreiber@mwe.com
Boston

Michael G. Morgan
+1 310 551 9366
mmorgan@mwe.com
Los Angeles, Silicon Valley

Ann Killilea
+1 617 535 3933
akillilea@mwe.com
Boston

Dr. Wolfgang von Frentz
+49 89 12712 157
wfrentz@mwe.com
Munich

Wilko van Weert
+32 2 282 35 65
wvanweert@mwe.com
Brussels

Camille Spegt
+33 1 81 69 14 94
cspegt@mwe.com
Paris

Leon C.G. Liu
+86 21 6105 0533
lliu@mwechinalaw.com
Shanghai

Jared T. Nelson
+86 21 6105 0513
jtnelson@mwechinalaw.com
Shanghai

McDermott Will & Emery

SPECIAL REPORT

The General Data Protection Regulation: Key Requirements and Compliance Steps for 2018

Table of Contents

The General Data Protection Regulation: Key Requirements and Compliance Steps for 2018

Many companies are in midst preparations for the General Data Protection Regulation (GDPR), which will become enforceable in all EU Member States on 25 May 2018 and will expand the territorial scope of EU data protection law.[1] The new regulation introduces numerous changes that will affect businesses' data processing operations. We review here steps for a risk based, prioritization approach to GDPR compliance and how companies can adjust their policies and practices on a pragmatic basis to help ensure compliance.

Some entities are not yet aware of the extent to which GDPR may be applicable to them. The GDPR expressly applies to organisations established outside the European Union that offer paid or free goods or services to EU data subjects or monitor EU data subjects' behaviour.[2] This gives the GDPR global reach, requiring compliance from organisations around the world.

For example, if a company was incorporated in another economic zone or jurisdiction, such as the United States or China, and did not have any subdivisions, units or affiliates in the European Union, it would still be subject to the GDPR in relation to services provided to data subjects in the European Union or if it monitored the behaviour of EU residents, including online.

Companies should consider taking actions with priority given to areas where non-compliance would be visible to individuals or regulators. EU bodies are constantly coming out with new or updated guidance on aspects of GDPR compliance. The Article 29 Working Party has issued a number of instructional papers[3] and noted that more will follow.[4] These will need to be tracked and absorbed. Doubtlessly, there will be continuing GDPR compliance activities beyond the May 25, 2018 date.

Steps to Compliance under the GDPR

STEP 1: MAPPING EU PERSONAL DATA AND PROCESSES, AND DETERMINING THE LEGAL BASIS FOR PROCESSING

DEFINITION OF PERSONAL DATA

Achieving compliance first requires covered organisations to determine what types of personal data they process as part of their business operations. The GDPR applies to "any information relating to an identified or identifiable natural person."[5] "Personal data" under the GDPR therefore refers to a large amount of information, including not only names, dates of birth, addresses and bank information, but also IP addresses,[6] cookie identifiers, Radio-Frequency Indentification (RFID) tags,[7] and factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of an individual, such as their height, salary, working hours, political opinions, medical history and fitness data. Even if the data being considered does not contain or comprise personal data, it will still be treated as personal data under the GDPR if it can be correlated with other data or databases that are available to the business and identify an individual.

Compared with the Directive, the GDPR imposes additional restrictions concerning the processing of children's data online,[8] extends the definition of "sensitive data" to include genetic data and biometric data processed for the purpose of

[1] GDPR will replace the current EU Data Protection Directive (95/46/EC) (Directive) and, to a large extent, the national data protection laws implementing the Directive.
[2] Article 3(1) GDPR; see also "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites" WP56 Article 29 Working Party.
[3] The Article 29 Working Party has issued final guidance already on data portability, data protection officers, choice of lead supervisory authority and fines, as well as draft guidance on data breach notification, consent and transparency, and automated decision making and profiling. See list at:http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
[4] http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48748 (December 2017)
[5] Article 4(1) GDPR.
[6] Notable Cases include C-582/14, *Breyer v. Bundesrepublik Deutschland* and French Civil Supreme Court, 1st Chamber, 3 November 2016, No. 15-22.595, P+B+I.
[7] Recital 30 GDPR.
[8] Article 8 GDPR states: "[T]he processing of the personal data of a child below the age of 16 in relation to the offer of information society services requires obtaining parental consent. Member States can provide by law for a lower age than 16, but cannot lower it below 13 years." Under Article 8, the controller is also required to make "reasonable efforts" to verify that consent has been given or authorised by the holder of parental authority over the child, taking into consideration available technology.

uniquely identifying a person,[9] and tightens the conditions for obtaining a data subject's "freely given, specific, informed and unambiguous" consent to the processing of his or her personal data.[10] The existing definition of personal data[11] will likely be more rigorously enforced and expansively interpreted by the European data protection regulators.

LAWFUL BASIS FOR PROCESSING

Under Article 5 of the GDPR, personal data must be processed lawfully, fairly and in a transparent manner, and must be collected for specified, explicit and legitimate purposes. Article 6 sets out the conditions which must be met to make the processing lawful.

There is now a requirement to understand the legal basis on which the business processes personal data. Particular attention should be paid to the updated provision relating to when consent can be used as a basis for processing,[12] and the conditions which permit processing based upon the legitimate interest of the data controller. Care should be taken to identify whether the company is a data controller or data processor as part of the data mapping exercise and with respect to any particular data processing, as this distinction is now very important. Under the current law, data processors do not have any statutory responsibility or liability. This position has changed under the GDPR, and companies that were primarily "processors" may now find that they have substantially increased liability. This concept is discussed again in the context of supply chain liability in Step 5.

Data mapping is important for several reasons: first, the additional factual detail concerning personal data that is processed and the processing that is taking place must be described in the revised privacy notice (see Step 2). These details must be added to the new accountability requirements (see Step 4) and are also necessary to understand changes that may be required to contracts with customers or suppliers (see Step 5).

There is a risk that the data mapping exercise can become too time consuming, and so care should be taken that appropriate resources are devoted to it but not at the expense of other critical GDPR tasks. If the compliance process is correctly structured, a company may proceed with further GDPR steps and return to complete the data mapping task at a later stage.

STEP 2: UPDATING DATA PROTECTION AND PRIVACY NOTICES

The GDPR sets out new provisions relating to transparency.[13] The European Commission was concerned with the need to make privacy notices simpler and easier to understand. The GDPR, however, requires much more information to be included in privacy notices, which are likely to be longer and more detailed.[14] The additional required detail includes the following:

- The purposes of the processing and the legal basis for the processing
- The recipients or categories of recipients of the personal data
- The details of the legitimate interests of the business, where the processing is based on those interests
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The details of the legal compliance mechanism which legitimises the export of personal data from the European Union, including how copies of the applicable contracts or other documents may be obtained
- The existence of automated decision-making, including profiling, and details of the logic involved and the consequences of that processing
- The existence of the data subjects' rights, including the right to have personal data corrected, deleted or restricted, as well as the right to data portability
- The data subjects' right to lodge a complaint with a supervisory authority

[9] Article 9 GDPR.
[10] Consent to the processing of personal data now requires either a statement or a clear affirmative action in order to be valid. It will be presumed not to be freely given "if the data subject has no genuine and free choice or is unable to refuse or withdraw consent without detriment" (Recital 42) or/and where "there is a clear imbalance between the data subject and the controller" (Recital 43). The data subject must have the right to withdraw his or her consent at any time (Article 7).
[11] "Opinion 4/2007 on the concept of personal data," WP136, Article 29 Working Party.
[12] The Article 29 Working Party has provided draft guidance "Guidelines on Consent under Regulation 2016/679," WP259, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849
[13] Articles 12 to 14 GDPR.
[14] Transparency is presently the subject of draft guidelines from the Article 29 Working Party, "Guidelines on transparency under Regulation 2016/679," WP260, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

Companies should start by cataloguing all of their data protection and privacy notices and ensuring that they have the appropriate scope. The notices then should be updated with the factual information that arises from Step 1, together with details of the additional rights which must be afforded to data subjects.

STEP 3: ACCOMMODATING THE RIGHTS OF DATA SUBJECTS

The GDPR introduces new, and strengthens existing, rights of data subjects, such as the following:

- The right to data portability, *i.e.*, the data subject's right to obtain the personal data that he or she has provided to a controller, in a structured, commonly used and machine-readable format, and to transmit it or have it transmitted to another controller.[15] This applies to data based either on a contract or on valid consent and is carried out by automated means such as databases or other IT systems operated by or on behalf of the controller. According to initial comments, the competent supervisory authorities may interpret the right of portability broadly.[16]
- The right to erasure, also known as the right to be forgotten.[17]
- The right to object to the processing of personal data without having to demonstrate "compelling legitimate grounds" for the objection, as was required under the Directive.[18]
- The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects the data subject.[19]
- Additional rights, such as the right to withdraw consent and the right to understand the basis for legitimising the export of personal data from the European Union.

Under the Directive, it has been possible to charge data subjects a fee before allowing them to exercise their right to access their personal data. It is currently contemplated that no fee will be permitted under the GDPR. If data subject requests increase considerably, additional resource or technology solutions may be necessary to accommodate them.

STEP 4: IMPLEMENTING ACCOUNTABILITY

The GDPR introduces various accountability obligations for controllers. The concept of accountability is part of a new bargain introduced under the GDPR. There is no longer a requirement for data controllers to make multiple filings to the supervisory authorities; instead, controllers must maintain an accountability database which keeps a record of all data processing activities.[20] This database must be kept up to date and must be in a form that allows a supervisory authority to inspect it at any time.[21] This also includes information about data breaches and remediation.[22]

PRIVACY IMPACT ASSESSMENT

The GDPR also requires controllers to conduct a privacy impact assessment prior to processing operations that are likely to result in a high risk to the rights and freedoms of individuals, such as profiling activities, large-scale processing of personal data, or systematic monitoring of a publicly accessible area on a large scale. This assessment must contain the following:

- A description of the expected processing
- An assessment of the processing's necessity and proportionality in relation to its purposes
- An assessment of the risks to the rights and freedoms of the data subjects
- The measures envisaged to address these risks, which may include safeguards, security measures and mechanisms to ensure the protection of the data[23]

Further, in amendments to supply contracts (see Step 5), controllers are beginning to require processors to provide them with a copy of the accountability information that relates to the processing of their data.

---

[15] Article 20 GDPR.
[16] The Article 29 Working Party considers that this right "covers data provided knowingly and actively by data subjects as well as the personal data generated by his or her activity:" "Guidelines on the right to portability," 13 December 2016, as revised on 5 April 2017, WP242 rev.01 http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.
[17] Article 17 GDPR.
[18] Article 21 GDPR and see http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963.
[19] See Article 22 of the GDPR, and guidance, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679," WP251, Article 29 Working Party, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963.
[20] Article 30 of the GDPR states that this obligation only applies to organisations that employ more than 250 people, unless the processing they carry out (1) "is likely to result in a risk to the rights and freedoms of data subjects," (2) "the processing is not occasional," or (3) the processing includes sensitive data. It is worth noting that the obligation to record processing activities also applies to processors, with regard to all categories of processing activities carried out on behalf of a controller.
[21] Article 30(4) GDPR.
[22] "Guidelines on Personal data breach notification under Regulation 2016/679," WP250, Article 29 Working Party, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47741
[23] Article 35 GDPR.

More generally, controllers will be required to implement appropriate technical and organisational measures to demonstrably ensure that processing is performed in compliance with the GDPR.[24] Such measures may consist "of minimising the processing of personal data, pseudonymising personal data as soon as possible, [and] transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing",[25] among other things.[26]

DATA PROTECTION OFFICER

One of the GDPR's major accountability innovations concerns the obligation to appoint a data protection officer (DPO) who is responsible for overseeing data processing operations. This requirement applies to entities whose core activities consist of either of the following:

- Processing operations which, by virtue of their nature, scope and/or purpose, require regular and systematic monitoring of data subjects on a large scale, such as the collection and subsequent processing of real time geo-location data of customers of an international fast food chain for statistical purposes[27]
- Processing, on a large scale, sensitive data or information in relation to criminal convictions and offences[28]

Public sector bodies must designate a DPO even if the aforementioned conditions are not met. The Article 29 Working Party has issued guidance for the functions of a DPO[29] which confirms that both controllers and processors might be required to appoint one. The DPO must monitor compliance with the GDPR, provide advice in respect of any data protection impact assessments and be a contact point for supervisory authorities. Companies may appoint external DPOs who may serve a number of different companies, similar to the current practice in Germany. In this case, particular attention should be paid to the terms and conditions in the contract with the DPO.

As of January 2018, according to a press release, the European Commission has earmarked 1.7 million euros to help fund data protection authorities and train data protection professionals, as well as another two million euros for member state-level information campaigns, particularly targeted at small businesses.[30]

STEP 5: MITIGATING DATA PROTECTION AND PRIVACY RISKS IN CUSTOMER CONTRACTS AND THE SUPPLY CHAIN

Under the Directive, there is a distinction between controllers and processors. Data controllers determine the purposes and means of the processing of personal data, and processors are the entities that process such personal data on behalf of the controllers.

One of the most significant changes in the GDPR is its imposition of statutory obligations on data processors. The new responsibilities for processors include implementing appropriate data security measures, notifying the controller of data breaches, maintaining records of processing activities carried out on behalf of the controller, and following the lawful instructions of the controller.

The Directive does not impose any statutory obligations on processors, and companies that have been able to characterise their activities as those of data processors have not had to comply with the Directive; they only have had to comply with the terms of the contract with the data controller.

With this change comes the risk that a data subject may sue a processor for failure to comply with its statutory obligations under the GDPR. The controller is likely to have a contract with the data subject which will frequently have limitation of liability provisions in the controller's favour. The processor will not have a contract with the data subject, and so its liability will not be limited. The processor can mitigate this risk by changing the terms of the contract with the controller and/or by having appropriate insurance.

[24] Article 24 GDPR.
[25] Recital 78 GDPR.
[26] The French data protection authority, the CNIL, has introduced a free software tool, in English, which can help companies undertake DPIAs. See https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil. The Article 29 Working Party has also introduced guidelines "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679," WP248rev.01, Article 29, Working Party, http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
[27] Guidelines on DPOs, 13 December 2016, revised on 5 April 2017, WP243 rev.01. http://ec.europa.eu/newsroom/document.cfm?doc_id=44100
[28] For example, with regard to the number of data subjects concerned, either as a specific number or as a proportion of the relevant population, the volume of data and/or the range of different data items being processed, the duration, or permanence, of the data processing activity, and even the geographical extent of the processing activity: Guidelines on DPOs, 13 December 2016, a revised on 5 April 2017, WP243 rev.01.
[29] "Guidelines on Data Protection Officers ('DPOs')," WP243, Article 29 Working Party, http://ec.europa.eu/newsroom/document.cfm?doc_id=44100
[30] https://iapp.org/news/a/commission-releases-extensive-gdpr-guidance/

Contracts between controllers and processors should be reviewed to ensure that they incorporate the additional provisions of the GDPR and appropriately allocate risk and liability in relation to actions which would infringe the GDPR.[31] The UK Information Commissioner's Office has produced preliminary guidance on this topic.[32]

Updating policies and systems to ensure that they are GDPR compliant may incur considerable cost. Change request mechanisms in a contract between controller and processor should be reviewed to ensure that it is clear which party will bear such cost.

Some processors may determine that they should be considered controllers under the GDPR. In this case further amendments to the contract would be required, including whether the parties should be considered joint controllers with shared responsibilities or alternatively co-controllers.

STEP 6: COMPLYING WITH NEW DATA BREACH NOTIFICATION OBLIGATIONS

The GDPR introduces a general data breach notification obligation and resolves uncertainty under the Directive. The Directive was silent on the issue of data breach notifications, only providing requirements for electronic communications operators (under EU Directive 2002/58, dated 12 July 2002, and EU Regulation 611/2013, dated 24 June 2011). This left Members States free to decide whether to impose data breach notification obligations. Some countries like Germany, Italy and the Netherlands choose to do so, but most did not, leaving conflicting notification obligations and standards in some European Union countries.

DEFINITION OF A SECURITY INCIDENT

Although there is often an immediate focus under the GDPR of a Personal Data Breach, the GDPR defines a wider concept first which is a security incident. A security incident is a failure to meet the cyber security requirements set out in Article 32. The definition is wider than that of a Personal Data Breach, and so not all security incidents will be notifiable, however a security incident will still be breach of the GDPR and may give rise to statutory and contractual liability.

DEFINITION OF PERSONAL DATA BREACH

Under the GDPR, a "personal data breach" is broadly defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."[33]

PROCESSOR NOTIFICATION TO THE DATA CONTROLLER

Processors must notify their controller without undue delay after becoming aware of a personal data breach. Strictly speaking, the processor is not itself directly responsible for notifying the supervisory authority or the data subjects affected by the breach. That responsibility falls to the controller. However, processors can be held liable if they do not notify the concerned controller promptly.[34]

DATA CONTROLLER NOTIFICATION TO THE SUPERVISORY AUTHORITY

In the event of a data breach, controllers must notify the competent supervisory authority if the rights and freedoms of individuals are at risk. Where there is doubt as to who the lead supervisory authority is, at minimum the local supervisory authority(ies) where the breach took place should be notified. [35] There is a key exception to this requirement: notification is not required where the personal data breach is unlikely to result in a risk to the rights and freedoms of the concerned data subjects.

In assessing the harm to the rights and liberties of data subjects, it will be necessary to consider "physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."[36]

Notification must be provided to the supervisory authority without undue delay and, where feasible, not later than 72 hours after the controller becomes aware of the data breach. Criteria for when an organization becomes "aware" of the breach allows for a short period of investigation to determine, to a

[31] Particular attention should be paid to Article 82(4) and 82(5) GDPR. These provisions give one controller or processor a statutory basis for a contribution claim against any other controller or processor involved in the same processing.
[32] https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf.

[33] Article 4(12) GDPR.
[34] Article 33(2) GDPR.
[35] "Guidelines on Personal data breach notification under Regulation 2016/679," WP250 at 15, Article 29 Working Party, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47741.
[36] Recital 75 GDPR.

reasonable degree of certainty, that a breach occurred and to establish the possible consequences for individuals.[37] If the notification to the supervisory authority is not made until after 72 hours, it must be accompanied by an explanation of the reasons for the delay.

A notification to the supervisory authority must include, at the very least, the following:

- A description of the nature of the breach, *i.e.*, the categories and approximate number of data subjects and personal data records concerned
- The name and contact details of the company's DPO or other contact point where more information can be obtained
- A description of the likely consequences of the data breach and the measures taken to address the breach, including measures to mitigate its possible adverse effects where appropriate

DATA CONTROLLER NOTIFICATION TO THE DATA SUBJECTS AFFECTED BY THE DATA BREACH

The data controller must inform the affected data subjects if the breach is likely to result in a high risk to their rights and freedoms. This may result, without limitation, where the breach:

- Concerns sensitive data
- Involves a large amount of personal data and affects a large number of data subjects
- May give rise to significant economic or social disadvantages such as discrimination, identity theft or damage to reputation

The European Data Protection Board, established by the GDPR and composed of the heads of the supervisory authorities of all Member States, is expected to issue guidelines, recommendations and best practices to help organisations determine under which circumstances a personal data breach is likely to result in a high risk to the rights and freedoms of individuals.[38]

Communication to the affected data subjects is not required in the following instances:

- The controller implemented appropriate technical and organisational protection measures to secure the concerned data, such as encryption.
- Following the breach, the controller took measures that ensure that the high risk to the rights and freedoms of the concerned individuals is no longer likely to materialise.
- A communication to individual data subjects would involve disproportionate effort. If the controller decides not to notify the affected data subjects for this reason, a public communication of the breach must be made instead.

When required, the notification to the affected data subjects must be done without undue delay. Such notification must essentially contain the same information as communicated to the supervisory authority and should be made "in clear and plain language."[39]

The supervisory authority can require the controller to communicate the personal data breach to affected data subjects.

Documenting Data Breaches

The controller is required to document any data breaches in order to enable the supervisory authority to verify whether the organisation complied with its obligations under the GDPR.

Sanctions

Failure to comply with the data breach notification rules may lead to administrative fines of up to €10 million (about $12 million) or 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher. Additionally,

---

[37] "Guidelines on Personal data breach notification under Regulation 2016/679," WP250 at 9, Art. 29 Working Party, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47741. ("This may raise the question of when a controller can be considered to have become "aware" of a breach. WP29 considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. This will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

***

After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place, and the possible consequences for individuals; a more detailed investigation can then follow").

[38] Article 70(h) GDPR.

[39] Article 34(2) GDPR.

data subjects will be entitled to receive compensation from the organisation for any damage suffered from the breach.

The Directive already allows sanctions for data breaches that are considered a violation of the obligation to ensure the security and confidentiality of the data. For example, the French supervisory authority recently sanctioned the French Socialist Party after the names, postal addresses, email addresses and phone numbers of more than 80,000 of its members were made public on the internet. The authority issued a warning against the Socialist Party, taking into consideration the large number of data subjects whose personal data was disclosed, the fact that sensitive data was concerned, and the Socialist Party's failure to use a sufficiently secure authentication system.[40]

A similar sanction was announced against a major French electronic communications company following a data breach that concerned the personal data of 1.3 million clients and prospects. The French Supreme Administrative Court confirmed this sanction in December 2015.[41]

While such sanctions may not seem very serious, the imposition of fines is likely to become the norm under the GDPR, which provides that "administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority".[42]

How to Prepare

Organisations must prepare to respond quickly to a data breach. The 72-hour notification requirement, even if it is only a preliminary report, will be difficult to satisfy, especially in situations where it is unclear whether a breach has actually occurred. Determining when the organization becomes "aware" of the breach is challenging and will depend on a myriad of circumstance. For example, some have read the Art. 29 Working Party guidance to suggest that the 72 hour period will run from when the forensic provider (if one has been engaged) provides results to the company, but this may not be a safe assumption.

Even when a breach has been identified, a case-by-case analysis will be required to determine whether it should be reported. This analysis involves assessing whether there is a risk to the rights and freedoms of the concerned individuals and determining who (supervisory authority and/or concerned individuals) should be notified. Where notification is required, organisations must carefully assess what information should be communicated.

Organisations should consider taking certain steps now to improve data security and prepare for responses to data breaches. Many US companies are already familiar with the process of data breach notification to authorities and individuals in the United States as a result of US data breach notification laws. They should be able to adapt their incident response procedure to the GDPR process without too much difficulty. Companies in the European Union, however, may have to create data breach and incident response policies and processes for the first time. These include the following:

- Identify an appropriate incident response team, including representatives from IT, security, legal, compliance, risk management, communications and customer service.
- Ensure that the members of the incident response team are sufficiently trained and prepared. Training should include occasional tabletop exercises that simulate a data breach and require the team to confront the types of issues they would face in an actual incident.
- Prepare an adequate incident response plan that provides guidance for critical incident response tasks, including identifying cyber incidents, assembling the incident response team, complying with the GDPR and other notification obligations, communicating internally and externally regarding the incident, making decisions about affected systems, conducting forensic investigations, and developing and implementing remediation strategies.
- Take appropriate technical measures in cooperation with IT specialists to render the organisation's data unintelligible in case of breaches.
- Review existing insurance coverage for cyber incidents to identify gaps in coverage, and remediate them.
- Ensure that data breach reporting obligations are

[40] *Commission Nationale de l'Informatique et des Libertés*, Decision No. 2016-315 of 13 October 2016.
[41] French Administrative Supreme Court, 30 December 2015, *Orange*, No. 385019.
[42] Recital 148 GDPR.

reflected in contracts entered into with processors.

The Article 29 Working Party has published further guidance on this subject which should be reviewed.[43]

Key Focuses

In addition to taking these compliance steps, covered organisations should pay particular attention to the following focus areas that are of crucial importance in the context of EU data protection.

FOCUS 1: CROSS-BORDER DATA TRANSFER RULES

The GDPR does not fundamentally change the current cross-border data transfer rules under the Directive. Controllers have been, and will continue to be, bound by strict rules when exporting personal data from the European Union.

ADEQUATE PROTECTION

The general principle holds that controllers may transfer personal data only to those countries outside of the European Union that offer "adequate protection," subject to certain derogations and exceptions.

Only the European Commission has the power to determine which countries offer adequate protection.[44] The GDPR contains more stringent criteria than the Directive in terms of what the Commission should consider when determining adequacy. Under the GDPR, the third country is expected to provide an adequate level of protection "essentially equivalent to that ensured within the Union." [45] Notably, the GDPR also provides that the Commission may consider as adequate not only a country, but also a specific sector or territory within a country.

The adequacy decisions that the Commission has rendered so far[46] will remain in force under the GDPR unless later repealed, amended or replaced. [47] Recent news reports indicate that the Commission is currently reviewing the existing adequacy decisions.[48]

EXEMPTIONS BASED ON APPROPRIATE SAFEGUARDS

The GDPR maintains the exemptions to the general principle already available under the Directive and adds new mechanisms.[49] Under the GDPR, controllers or processors will be able to transfer data to entities outside the European Union in the following circumstances:

- Controllers and processors adopt internal binding corporate rules for data exchanges with affiliated companies, approved by the relevant supervisory authority, which define the group's global policy in terms of the international transfer of personal data within the group to entities located in countries that do not provide adequate protection.[50]
- In the absence of binding corporate rules, EU-based controllers or processors enter into standard contractual clauses with controllers and processers receiving the personal data outside the European Union on the basis of model contracts adopted or approved by the European Commission.
- In the absence of binding corporate rules and standard contractual clauses, controllers and processers receiving personal data outside the European Union make a binding and enforceable commitment to adhere to standards included in a code of conduct [51] or a certification scheme [52] approved by a supervisory authority, both newly introduced by the GDPR.

A significant improvement under the GDPR is that national supervisory authorities no longer need to authorise the use of all these mechanisms before companies can start transferring personal data outside the European Union. Binding corporate rules, the codes of conduct and the certification schemes will still require approval, however. This change will help streamline the process and enable companies to transfer data abroad more efficiently.

---

[43] See "Guidelines on Personal data breach notification under Regulation 2016/679, wp250" Article 29 Working Party http://ec.europa.eu/newsroom/document.cfm?doc_id=47741.
[44] Article 45 GDPR.
[45] Recital 104 GDPR.
[46] The Commission has so far recognised the following countries as providing adequate protection: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm. Reports have indicated that Japan and South Korea have applied and are now also being considered for adequacy recognition. The Art. 29 Working Party has recently issued guidance on relevant factors under GDPR for adequacy decisions. "Adequacy Referential (updated)," 17/EN WP254, 28 Nov. 2017. https://iapp.org/media/pdf/resource_center/wp29-Adequacy-referential.pdf.
[47] Article 46 GDPR.
[48] See http://www.euractiv.com/section/data-protection/news/commission-conducting-review-of-all-foreign-data-transfer-deals/.
[49] Article 46 GDPR.
[50] Article 47 GDPR. It should also be noted that Binding Corporate Rules are now expressly recognised in the GDPR as a legitimate method by which to transfer data abroad.
[51] Article 40 GDPR.
[52] Article 42 GDPR.

In a development not mentioned in the GDPR, on 12 July 2016, the Commission approved the Privacy Shield Framework, a new mechanism permitting companies to transfer data to the United States, effectively replacing the Safe Harbour. Personal data can now be transferred to the United States if the recipient company is registered with the US Department of Commerce and commits to compliance with the Privacy Shield requirements.

Companies should be aware, however, that both the Privacy Shield Framework and the model clauses have been challenged in court proceedings. At the time of writing, there are several cases on the Privacy Shield before the General Court of the European Union.[53] The parties in these cases allege that the Privacy Shield Framework does not ensure a level of protection of fundamental rights substantially equivalent to that guaranteed in the European Union. In addition, court proceedings in Ireland are questioning the ability of companies to rely on standard contractual clauses as a compliance mechanism.[54] The Irish High Court referred the validity of the model clauses to the Court of Justice of the European Union (CJEU). Model clauses will be adequate in the interim, until the Court of Justice reaches a decision on this case.

LIMITED DEROGATIONS

Aside from the previously described exemptions, which are intended to be widely used, the GDPR includes a list of derogations that permit, in very strict and limited circumstances, the transfer of data to non-EU countries that do not provide an adequate level of protection.

Some of these derogations were already provided for under the Directive, but the GDPR adds a new derogation[55] for non-repetitive transfers involving a limited number of data subjects where the transfer is necessary for the purposes of compelling legitimate interests of the controller that are not overridden by the interests of the data subject. In such a case, the controller must inform the supervisory authority and the data subjects of the transfer.[56]

Transfers Not Authorised by EU Law

The GDPR makes it clear that data transfers outside the European Union on the grounds of a legal requirement from a foreign country are generally not permitted, unless those transfers are subject to appropriate international agreements.[57]

Sanctions

Cross-border transfers of personal data without respecting appropriate safeguards may lead to administrative fines of up to €20 million (about $24 million) or 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

For example, the French supervisory authority recently imposed a fine of €30,000 on BrandAlley for having, among other things, transferred personal data outside the European Union without respecting appropriate safeguards.[58]

How to Prepare

Companies should assess whether their current data transfer mechanisms comply with the GDPR or whether another method should be employed consistent with the GDPR.

Controllers and processors in the United States that are likely to receive data originating from the European Union should consider registering for the Privacy Shield with the US Department of Commerce if they have not already done so. Please click here for more information on McDermott's Privacy Shield How-To-Kit.

In making their data privacy decisions, companies should assess whether they wish to invest in more expensive long-term solutions, such as the binding corporate rules, or keep using what may turn out to be short-term approaches, such as those on standard contractual clauses, depending on the outcome of cases determined at the CJEU.

[53] Case T-670/16, *Digital Rights Ireland v. Commission*, Action brought on 16 September 2016; Case T-738/16, *La Quadrature du Net and others v. Commission*, Action brought on 25 October 2016.
[54] Record No. 2016/4809 P, *Data Protection Commissioner v. Facebook Ireland Ltd. & Maximilian Schrems*.
[55] Actually resulting from the Article 29 Working Party previous interpretations: Working Document, 25 November 2005, WP114.
[56] Article 49 GDPR.
[57] Article 48 GDPR.
[58] *Commission Nationale de l'Informatique et des Libertés*, Decision No. 2016-204 of 7 July 2016.

FOCUS 2: ANTICIPATING SANCTIONS, ENFORCEMENT AND LIABILITY

As under the Directive, supervisory authorities will be provided with extensive investigative powers under the GDPR, such as the power to conduct audits, obtain access from controllers and processors to all personal data necessary to fulfil the supervisory role, and obtain access to the premises of controllers and processors. Such investigative activities can cause business disruption.

The GDPR also endows supervisory authorities with significant corrective powers, such as the power to take the following actions:

- Issue warnings
- Order controllers and processors to comply with a data subject's request to exercise his or her rights
- Issue a temporary ban on processing operations
- Order the suspension of data flows to a recipient in a third country
- Withdraw a certification[59]

Most importantly, supervisory authorities will have the power to impose hefty fines in cases of violation of the GDPR. As noted, the transfer of personal data outside the European Union without having appropriate safeguards in place may lead to an administrative fine of up to €20 million or 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

When setting the amount of the fine, supervisory authorities will need to consider, among other things:

- The nature, gravity and duration of the infringement
- The intentional or negligent character of the infringement
- Any action taken to mitigate the damage suffered
- The degree of cooperation of the controller or processor with the supervisory authority
- The type of personal data affected
- Aggravating or mitigating factors, such as financial benefits gained by the controller or processor[60]

[59] Article 58 GDPR.
[60] Article 83 GDPR.

It is too early to tell how the supervisory authorities will apply these sanctions, but it seems inevitable that there will be different approaches in different Member States, which may lead to some legal uncertainty. Given the wide range of enforcement and sanctioning powers provided by the GDPR to supervisory authorities, it is fair to say that sanctions are likely to increase and supervisory authorities will be less likely to be lenient with violators.[61]

Private Legal Actions and Quasi-Class Actions

There are two areas of particular concern regarding private legal actions. First, not-for-profit bodies, organisations or associations may now lodge complaints and bring legal actions on behalf of data subjects.[62] This change will introduce a quasi-class-action ability against corporations and some law firms may offer to represent these not-for-profit bodies on a contingent fee basis to allow the claim to proceed.[63]

Second, under the GDPR there is a reversal of the burden of proof: "A controller or processor shall be exempt from liability . . . if it proves that it is not in any way responsible for the event giving rise to the damage".[64] The chances of private legal actions against companies are greatly increased, as is the level of risk for companies that have not implemented a comprehensive accountability solution (see Step 4). This risk is particularly acute for legacy data, where it is often difficult to determine the conditions upon which it was collected.

FOCUS 3: DEALING WITH SUPERVISORY AUTHORITIES

Under the Directive, the national data protection authority acting as competent "supervisory authority" is responsible for monitoring and enforcing the application of EU data protection rules in each Member State. This obligation will continue to apply under the GDPR, subject to new rules concerning the

[61] Further guidance has been produced by the Article 29 Working Party, "Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679," WP253 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889
[62] Article 80 Recital 142 GDPR.
[63] Of interest, on January 25, 2018, the European Court of Justice ruled that Mr. Schrems may bring an individual action in Austria against Facebook Ireland, but cannot bring claims on behalf of other users in a class action lawsuit. The ECJ held that Mr. Schrems is free to litigate against Facebook as a consumer, despite using the services on behalf of his professional interests, but he can bring a claim only for himself and not for others. He had attempted to bring an action on behalf of himself as a consumer and on behalf of 25,000 consumer users claiming damages for each. *See Maximilian Schrems v. Facebook Ireland Limited (Case C-498/16) (January 25, 2018*), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0498.
[64] Article 82(3) GDPR.

competencies of the supervisory authorities and the cooperation between them.

As a general rule, each supervisory authority will be competent "for the performance of the tasks assigned to and the exercise of the powers conferred on it . . . on the territory of its own Member State." [65] For example, the French supervisory authority will be competent where data processing affects individuals in France, or where the processing is carried out by French authorities or by a controller or processor established in the context of its activities in France.

The GDPR also introduces a one-stop-shop system with respect to the processing of personal data connected to multiple Member States. It applies either to controllers or processors having establishments in more than one Member State, or to controllers or processors whose establishment located in a single Member State substantially affects data subjects in more than one Member State.[66] In these cases, the supervisory authority of the main establishment or of the single establishment will be competent to act as lead supervisory authority for the cross-border processing within the European Union.

The lead supervisory authority will be required to cooperate with the other relevant supervisory authorities in the decision-making process. All relevant supervisory authorities will need to agree upon joint decisions following a complex process described in Article 60 of the GDPR.

Apart from this rule, each supervisory authority will be competent to handle a complaint lodged with it, or a possible violation of the GDPR, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in this State. The final decision as to who will handle the matter in these cases rests with the lead supervisory authority. [67] The Article 29 Working Party has issued further guidance in relation to the role of the lead supervisory authority.[68]

European Law versus National Law

The GDPR will be directly applicable and enforceable in all EU Member States, and will therefore to a large extent harmonise personal data protection law throughout the European Union. It does not, however, prohibit Member States from adopting national legislation.

The GDPR notes that "Member States have several sector-specific laws in areas that need more specific provisions."[69] This is specifically the case where the processing is necessary for compliance with a legal obligation, for the performance of a task carried out in the public interest or where sensitive data is concerned. Organisations active in sectors with additional rules, such as the health sector, should therefore keep an eye on national legislation in addition to the general personal data protection rules set forth in the GDPR.

Moreover, Member States may institute specific national laws governing certain areas not covered by the GDPR, such as "the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities,"[70] or "the processing of personal data of deceased persons."[71]

In certain limited circumstances, Member States may also derogate from the GDPR. For example, "if the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established."[72]

FRANCE

In France, specific rules apply to the hosting of personal health data. Under Article L. 1111-8 of the French Public Health Code, only entities that hold a specific authorisation granted for a three-year period by the Minister of Health can host personal health data collected in France through prevention, diagnosis and care activities, on behalf of health care establishments or health care professionals, or on behalf of the patients themselves. This obligation applies wherever the data are stored.

[65] Article 55 GDPR.
[66] Article 4(23) GDPR.
[67] Article 56(3) GDPR.
[68] "Guidelines on The Lead Supervisory Authority," WP244rev.01_en, Article 29 Working Party, http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.

[69] Recital 10 GDPR.
[70] Recital 20 GDPR.
[71] Recital 27 GDPR.
[72] Recital 56 GDPR.

Hosting personal health data without authorisation is punishable by up to three years imprisonment and a €45,000 fine.

The authorisation procedure will be replaced by an accreditation system, according to which the hosting provider will only have to be certified by a third party by 1 January 2019.

GERMANY

Germany passed an amendment on 12 May 2017, that brought the Federal Data Protection Act (*Bundesdatenschutzgesetz*, or BDSG) in line with the GDPR.[73] Together with the GDPR, the BDSG will become fully applicable on 25 May 2018.

In addition to repealing the provisions of the previous version of the BDSG that either duplicate or contradict the GDPR, the amendment bill supplements the GDPR based on several of the GDPR's opening clauses. For example, the amendment bill introduces specific rules on the processing of personal data in the context of employment, for research and statistics purposes, with respect to consumer loans, and in relation to scoring and credit reporting agencies.

The revised BDSG continues to implement Germany's traditionally strict policy on the designation of data protection officers by requiring, among other things, that businesses with 10 or more employees regularly involved in the processing of personal data by computers or other automated means appoint a data protection officer.

The revised BDSG also creates several exemptions from the rights to information, access and erasure that data subjects generally enjoy under the GDPR. While it was argued by data protection experts that some of these exemptions go beyond what is permitted by the opening clauses of the GDPR, the German legislature considered them necessary to protect particular business or public interests.

The enforcement scheme of the revised BDSG not only includes the administrative fines set forth in the GDPR, but also establishes personal criminal liability for violations knowingly committed in exchange for money, for the purposes of achieving personal gain (either for oneself or a third party) or in order to harm a third party. Respective criminal sanctions include incarceration for up to three years and financial penalties.

In addition to the general data protection regime codified in the BDSG, German law includes sector-specific provisions set forth in the Telecommunications Act (*Telekommunikationsgesetz*), the Telemedia Act (*Telemediengesetz*) and the Social Security Code (*Sozialgesetzbuch*), to name just a few. These provisions are yet to be adjusted or repealed in light of the GDPR and the proposed ePrivacy Regulation discussed subsequently in this article. While this process must be completed before the GDPR or the proposed ePrivacy Regulation becomes fully applicable, its outcome is currently unpredictable.

ITALY

Companies active in the Italian health sector must comply with specific rules set out by the Italian Data Privacy Authority under a variety of authorisations, such as general authorisation No. 2 of 2016 on the treatment of data concerning health and sexual life, general authorisation No. 8 of 2016 on the treatment of genetic data, and general authorisation No. 9 of 2016 on the treatment of data for research purposes. These authorisations will expire on 24 May 2018, but are likely to be renewed to take into account the (limited) adjustments required by the GDPR's entry into force.

Health care companies are also subject to special rules, such as those set out in guideline No. 273 of 2016 on electronic health records and health files, which requires the implementation of suitable authentication and authorisation systems to limit access to health data. Each action should be traceable, and access should be granted for no longer than is necessary to carry out the purpose.

UNITED KINGDOM

In March 2017, the United Kingdom served two years' notice, under Article 50 of the Treaty on the European Union, of its intention to leave the European Union in 2019 (the so-called Brexit), less than 12 months after the GDPR comes into effect.

The UK Government has stated its commitment to ensuring "a world-class regime for protecting personal data" and maintaining the ability for data to be shared with EU Member States and internationally after Brexit. It might be anticipated, therefore, that any new UK data protection law will adopt equivalent standards to those in the GDPR.

[73] *Gesetz zur Anpassung des Datenschutzrechts an die Verordnung* (EU) 2016/679 *und zur Umsetzung der Richtlinie* (EU) 2016/680 (*Datenschutz-Anpassungs- und Umsetzungsgesetz* EU – DSAnpUG-EU).

The GDPR will be directly applicable to the United Kingdom, alongside other EU Member States, until March 2019. In order to implement the GDPR, the UK Government has proposed a Data Protection Bill[74], which is presently being debated in the House of Lords and the House of Commons. Fundamentally, the Bill seeks to do two key things:

- Confirm that the provisions of the GDPR will, to all practical purposes, remain in force in respect of the United Kingdom once it has left the European Union
- Take advantage of provisions in the GDPR which permit more specific rules to be introduced in specific areas, most notably employment

The Bill also seeks to address certain processing that does not currently fall within EU law (for example, in relation to immigration), impose internationally recognised data protection standards on the intelligence services, and implement the European Union's Law Enforcement Directive.

Upon Brexit, companies in the United Kingdom that do business in Europe will need to comply with the UK version of the GDPR under the Data Protection Act, as well as the provisions of the GDPR as they apply to non-EU territories. The European Commission has warned that upon Brexit, companies should ensure that they have an adequate basis for transferring personal data from the remaining EU Member States to the United Kingdom.[75]

BELGIUM

The GDPR largely confirms Belgium's existing data protection principles, which will continue to be supervised by the Privacy Commission. Special rules currently exist for the protection of sensitive personal data (data that reveals racial or ethnic origin, political opinions, religious beliefs, *etc.*), health-related personal data, and data related to litigation that has been submitted to courts, tribunals or judicial bodies.

There are exceptions under which sensitive data can be processed. For example, health-related data can be processed if necessary to prevent a specific danger or punish a particular criminal offence, or to promote and protect public health. The rules governing judicial data are stricter; judicial data can only be processed in exceptional cases, such as under the supervision of a public authority or by lawyers for the defence of their clients' rights.

The Belgian Government is still working on proposals to support and complement the GDPR, which will be directly applicable in Belgium.

THE NETHERLANDS

The Dutch Implementation Act contains a legal framework for implementing the GDPR in the Netherlands on the same day the GDPR enters into force. The Implementation Act states that, while the GDPR will replace the existing Dutch Personal Data Protection Act, the Government's position is one of "policy neutrality," meaning national law will be maintained insofar as possible in light of the incoming regulation.

Because the GDPR has direct effect in all Member States, the Implementation Act does not include its provisions verbatim, but instead complements the GDPR, thereby creating a layered legal framework.

The national provisions mainly deal with the administrative framework concerning the Dutch Data Protection Act and the processing of biometric data. Biometric data processing will be allowed only if such processing "is done to identify the data subject where such identification is necessary and proportional for the legitimate purposes of the controller or a third party." This exception is the Netherlands' specific implementation of Clause 9 of the GDPR, which allows Member States to apply exceptions if certain conditions are met.

[74] See https://services.parliament.uk/bills/2017-19/dataprotection.html.
[75] *Withdrawal of the United Kingdom from the Union and EU Rules in the field of Data Protection* http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245

LUXEMBOURG

The Luxembourg Parliament is establishing legislation that aims to abolish certain authorisation regimes currently in place under the 2002 Luxembourg Data Protection Act in order to facilitate the implementation of the GDPR and reduce the workload of the Luxembourg data protection authority (the CNPD). The authorisation regimes it is abolishing are as follows:

- Regime for interconnection, *i.e.*, the correlation of data that are processed for a given purpose with data processed for another purpose and/or by another controller.
- Regime for surveillance, *i.e.*, the non-occasional observing, collecting or recording of personal data. Although the GDPR allows Member States to adopt stricter rules in the context of employment relationships, the authorisation requirement for this type of processing is likely to disappear in the near future.
- Regime for credit and solvency related personal data, *i.e.*, financial data processing carried out by controllers that are neither financial nor insurance service providers. The abolition of this regime will likely be welcomed by undertakings acquiring distressed consumer debt from foreign banks via Luxembourg for special purpose vehicles.
- Regime for transfer of data to non-EU countries. Under the new law, transfers to non-EU countries will no longer require notification if they are based on standard contractual clauses.

The ePrivacy Regulation

The ePrivacy Regulation is the next step in the modernisation of the EU data protection framework. The currently applicable ePrivacy Directive 2002/58/EC, which aims to ensure respect for private life, confidentiality of communications and protection of personal data in the electronic communications sector, "particularised and complemented" the Directive concerning electronic communications data.[76]

Following the GDPR, it will become necessary to update the ePrivacy legislation to align with the new data privacy rules. Following a public consultation held from April to July 2016, the Commission published a Proposal for an ePrivacy Regulation that would replace the ePrivacy Directive on 10 January 2017.

One of the most significant changes brought by the proposal concerns the scope of the ePrivacy obligations. The new ePrivacy Regulation would apply to all providers of electronic communications services, including over-the-top service providers such as WhatsApp, Skype and Facebook Messenger, which are not currently covered by the ePrivacy Directive and therefore are not subject to the same security and privacy obligations as traditional electronic communications providers. The ePrivacy Regulation would also apply to non-EU providers that provide electronic services, even for free, to EU residents.

The proposed Regulation strictly limits the processing of electronic communications data, including both the content of the communications and its metadata, *e.g.*, the receiver, the timing, the location and duration of the call, and websites visited.

Under the proposed Regulation, electronic communications data that includes both content and metadata may be processed only if it is necessary to achieve the transmission of the communication or to maintain or restore the security of electronic communications networks and services.

Electronic communications content can be processed only under the following conditions:

- For the sole purpose of the provision of a specific service to an end user, if the end user concerned has given his or her consent to the processing and if that processing is necessary to provide the service.
- For a specific purpose that cannot be fulfilled by processing information that is made anonymous, only if all end users concerned have given their consent to the processing of the content and if the company complies with the GDPR obligation to consult the relevant data protection authority prior to the processing.[77]

The proposal provides specific rules for the processing of metadata. Metadata can be processed in the following circumstances:

- If it is necessary to meet mandatory quality of service requirements

[76] Article 1(2) of Directive 2002/58/EC.

[77] Article 36 GDPR.

- If it is necessary for billing, calculating interconnection payments, or detecting or stopping fraudulent or abusive use of, or subscription to, electronic communications services
- If the end user concerned has given his or her consent to the processing of metadata for a specific purpose or purposes, provided such purposes could not be fulfilled by processing information that is made anonymous

The proposal, which also includes provisions on cookies and unsolicited electronic communications, is the first step in the legislative process towards the adoption of the new ePrivacy Regulation. While this process could last several years and will certainly involve significant amendments to the current text, electronic communications providers should be aware of its potential impact on their activity.

Conclusion

The important changes brought by the GDPR and the ePrivacy Regulation require action by organisations both inside and outside the European Union to ensure compliance with this far-reaching privacy legal framework. The timing of the new requirements can also create an opportunity for a unified global assessment and response to other significant changes that are happening in other key jurisdictions. Compliance is even more urgent given that the GDPR provides for large penalties in cases of infringement.

If you have questions regarding the GDPR or would like to discuss how it affects you, please contact your regular McDermott lawyer or any of the authors listed in this article.

Authors:

Ashley Winton
+44 20 7577 6939
awinton@mwe.com
London

Romain Perray
+33 1 81 69 15 27
rperray@mwe.com
Paris

Sabine Naugès
+33 1 81 69 15 06
snauges@mwe.com
Paris

Paul McGrath
+44 20 7577 6914
pmcgrath@mwe.com
London

Mark E. Schreiber
+1 617 535 3982
mschreiber@mwe.com
Boston

Michael G. Morgan
+1 310 551 9366
mmorgan@mwe.com
Los Angeles, Silicon Valley

Ann Killilea
+1 617 535 3933
akillilea@mwe.com
Boston

Dr. Wolfgang von Frentz
+49 89 12712 157
wfrentz@mwe.com
Munich

Wilko van Weert
+32 2 282 35 65
wvanweert@mwe.com
Brussels

Camille Spegt
+33 1 81 69 14 94
cspegt@mwe.com
Paris

Leon C.G. Liu
+86 21 6105 0533
lliu@mwechinalaw.com
Shanghai

Jared T. Nelson
+86 21 6105 0513
jtnelson@mwechinalaw.com
Shanghai

For more information about McDermott Will & Emery visit www.mwe.com

Office Locations

BOSTON
28 State Street
Boston, MA 02109
USA
Tel: +1 617 535 4000
Fax: +1 617 535 3800

BRUSSELS
Avenue des Nerviens 9-31
1040 Brussels
Belgium
Tel: +32 2 230 50 59
Fax: +32 2 230 57 13

CHICAGO
444 West Lake Street, Suite 4000
Chicago, IL 60606
USA
Tel: +1 312 372 2000
Fax: +1 312 984 7700

DALLAS
2501 North Harwood Street, Suite 1900
Dallas, TX 75201-1664
USA
Tel: +1 214 295 8000
Fax: +1 972 232 3098

DÜSSELDORF
Stadttor 1
40219 Düsseldorf
Germany
Tel: +49 211 30211 0
Fax: +49 211 30211 555

FRANKFURT
Feldbergstraße 35
60323 Frankfurt a. M.
Germany
Tel: +49 69 951145 0
Fax: +49 69 271599 633

HOUSTON
1000 Louisiana Street, Suite 3900
Houston, TX 77002
USA
Tel: +1 713 653 1700
Fax: +1 713 739 7592

LONDON
Heron Tower
110 Bishopsgate
London EC2N 4AY
United Kingdom
Tel: +44 20 7577 6900
Fax: +44 20 7577 6950

LOS ANGELES
2049 Century Park East, 38th Floor
Los Angeles, CA 90067
USA
Tel: +1 310 277 4110
Fax: +1 310 277 4730

MIAMI
333 Avenue of the Americas, Suite 4500
Miami, FL 33131
USA
Tel: +1 305 358 3500
Fax: +1 305 347 6500

MILAN
Via dei Bossi, 4/6
20121 Milan
Italy
Tel: +39 02 78627300
Fax: +39 02 78627333

MUNICH
Nymphenburger Str. 3
80335 Munich
Germany
Tel: +49 89 12712 0
Fax: +49 89 12712 111

NEW YORK
340 Madison Avenue
New York, NY 10173
USA
Tel: +1 212 547 5400
Fax: +1 212 547 5444

ORANGE COUNTY
4 Park Plaza, Suite 1700
Irvine, CA 92614
USA
Tel: +1 949 851 0633
Fax: +1 949 851 9348

PARIS
23 rue de l'Université
75007 Paris
France
Tel: +33 1 81 69 15 00
Fax: +33 1 81 69 15 15

SEOUL
18F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
Tel: +82 2 6030 3600
Fax: +82 2 6322 9886

SHANGHAI
MWE China Law Offices
Strategic alliance with
McDermott Will & Emery
28th Floor Jin Mao Building
88 Century Boulevard
Shanghai Pudong New Area
P.R.China 200121
Tel: +86 21 6105 0500
Fax: +86 21 6105 0501

SILICON VALLEY
275 Middlefield Road, Suite 100
Menlo Park, CA 94025
USA
Tel: +1 650 815 7400
Fax: +1 650 815 7401

WASHINGTON, DC
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001
USA
Tel: +1 202 756 8000
Fax: +1 202 756 8087

McDermott Will & Emery

Boston Brussels Chicago
Dallas Düsseldorf Frankfurt Houston London
Los Angeles Miami Milan Munich
New York Orange County Paris
Seoul Silicon Valley Washington, DC

Strategic alliance with MWE China Law Offices (Shanghai)

www.mwe.com