MORRISON FOERSTER

# The EU General Data Protection Regulation: A Primer for International Business

Alex van der Wolk and Sotirios Petrovas

03/23/2016

Privacy + Data Security

Client Alert

## 1. Introduction

The European Union will soon enact the General Data Protection Regulation (GDPR) to regulate the collection and processing of personal information of EU individuals. When the GDPR comes into effect in 2018, it will replace the 1995 Data Protection Directive (95/46/EC) (the "Directive") and introduce new obligations that will impact companies around the globe.

Key changes include:

- The GDPR will apply not only to companies established in the EU, but to all companies that target EU markets or consumers.
- Penalties for non-compliance will reach unprecedented heights with new maximum fines of EUR 20 million or 4% of annual worldwide revenue.
- EU legislators have introduced significant compliance burdens such as recordkeeping obligations and mandatory privacy impact assessments (PIAs) and, under the accountability principle, companies will have to be able to demonstrate compliance upon request.
- New individual rights include the right to be forgotten and the right to data portability.
- Binding Corporate Rules (BCRs) are formally recognized as an international transfer mechanism.
- Mandatory breach notification will be established for all of the EU Member States.

## 2. Overview of Key Concepts and Principles

Both the Directive and the GDPR impose obligations with regard to virtually *all* processing of personal data. *Personal data* includes any information relating to an identified or identifiable individual. The GDPR specifically includes location data and online identifiers as personal data (Article 4(1)).[1] Heightened restrictions continue to be imposed on processing of sensitive data, which under the GDPR also include genetic data and biometric identification data (Article 9). The obligations under the GDPR focus primarily on companies that are "data controllers" who make decisions regarding how personal data are collected, used and shared, but the GDPR also

introduces new obligations for companies that are only data processors. Data processors will have direct responsibility for compliance with requirements relating to cross-border transfers, security, appointing data privacy officers (DPOs), and recording their processing activities. The GDPR's regulatory framework is guided by a set of principles, which include: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; data security; and accountability (Article 5). The following sections highlight aspects of the implementation of these principles.

**3. Conditions for Collection and Use**

**Legal Basis for Processing.** Under the GDPR companies must have a *legal basis* or "good reason" to process personal data, such as consent of the individual; necessity to perform a contract; compliance with a legal obligation; or a legitimate interest of the company that outweighs the privacy rights of the individuals. While these legal bases are very similar to the rules under the Directive, some legal bases such as consent and legitimate interest will change under the GDPR (Article 6).

**Consent.** The GDPR defines consent as a "freely given, specific, informed and unambiguous indication" in the form of a statement, or "clear affirmative action," and prescribes detailed conditions for its validity (Articles 4(8), 7). For example, individuals can withdraw consent at any time (Article 7(3)). Furthermore, the provision of a service cannot be made conditional on the individual providing his/her consent to certain processing, if that processing is not necessary for the performance of the contract (Article 7(4)) (for instance, when a service is only available if the individual also consents to analytics or advertising, the consent will be invalid). If sensitive data or data relating to children (under the ages of 13 to 16, depending on the Member State) are involved, further restrictions apply, requiring *explicit* consent and parental consent, respectively. This means that companies must provide detailed information to individuals when collecting their data in order for the consent to be valid.

**Legitimate Interest.** The difficulty of complying with the requirements of consent often causes companies to look for alternative grounds for processing. Under the GDPR, a company's interest must be weighed against the rights of individuals. There are some specific examples given in the GDPR of a company's legitimate interest including fraud prevention, information security, and intra-group disclosures (Recitals 38-39).

**Purpose Limitation and Big Data.** According to the principle of purpose limitation, personal data may only be processed for the purposes specified when the personal data were collected. This is a challenge for companies wishing to employ Big Data analytics using data that were previously collected. The GDPR introduces an exception which allows for processing if the purpose is not "incompatible" with the original purpose, and a set of factors to assess (in)compatibility. The factors include the link between the purposes for which the data were collected and the intended new purposes; the relationship between the individual and the company; the nature of the personal data; the "possible consequences" for individuals; and the existence of safeguards such as encryption or pseudonymization (Article 6(3a)).

**4. New Individual Rights and Limits on Profiling**

The GDPR maintains the individual rights of access, correction, deletion, blocking, and objection and introduces new rights, such as the right to be forgotten and the right to data portability. Furthermore, it aims to regulate the use of profiling by granting individuals a right not to be subject to decisions based solely on automatic decision making.

**The Right to Be Forgotten.** The "new" right to be forgotten is best understood as a more detailed implementation of the right to request that personal data be deleted. While the idea of the right to be forgotten is mostly intuitive in the context of search engines and the retrievability of potentially old information on the Internet, the right applies to all data controllers. However, the right to be forgotten is not unlimited. Exemptions apply if the processing is deemed necessary for the exercise of freedom of expression, compliance with a legal obligation, public interests such as public health, scientific or historic research, or the establishment or defense of legal claims (Article 17(3)). It is not yet clear how the right to be forgotten will be interpreted and implemented outside the search context.

**The Right to Data Portability.** With the right to data portability, the EU aims to provide a way for consumers to take their data from one service provider to another. Individuals will be able to request a copy of their personal information in a structured and commonly used electronic ("machine readable") format, and—where feasible—request that the data be transferred between companies directly. However, companies need not implement systems that are technically compatible to facilitate such direct transfers. Furthermore, the portability right only applies with regard to information that was obtained on the basis of consent or as necessary for the performance of a contract, but not where information was obtained on other grounds (e.g., compliance with a legal obligation).

**Limitations on Profiling.** Profiling has been a hotly debated topic. The GDPR includes a right with regard to certain decisions companies may make as a result of profiling. Thus Article 20 limits decisions based *solely* on automated processing (including profiling) which produce a legal or similarly significant effect concerning an individual. In particular, to analyze or predict performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. Examples of profiling activities named by the GDPR include automatic refusal of an online credit application and e-recruiting practices without human intervention. Important questions remain regarding the scope of this provision: What effects are significant enough to trigger this provision? When is a decision based *solely* on profiling? Automated decisions may still be made when necessary for the performance of a contract with an individual, or with explicit consent, although additional restrictions may apply.

**5. International Effects**

**Applicability Regime.** The GDPR will apply to the processing of personal data by controllers and processors that are established in the EU, but also to companies outside the EU that (a) offer goods or services to individuals located in the EU (regardless of whether payment is sought) or (b) monitor behavior of individuals in the EU (as far as that behavior takes place in the EU). The "offering of goods or services" criterion requires some form of targeting of individuals in the EU. The mere accessibility of a website from the EU, or the use of a language that is also used in Europe (where such language is also the language of the controller's country) does not necessarily lead to applicability. A combination of factors may lead to the determination that the company is targeting EU individuals, such as the ability to order goods and services in an EU language, payment options in EU currencies, and providing local content. The "monitoring behavior of individuals" criterion requires that such behavior takes place in the EU, including the tracking and the profiling of EU individuals on the Internet.

**Cross-Border Transfers and Binding Corporate Rules.** EU data protection law prohibits transfers of personal data to non-EU countries that do not provide for an "adequate level of personal data protection" without

individuals' explicit consent, unless "appropriate safeguards" are in place. In addition to continuing to recognize the EU-approved Standard Contractual Clauses, the GDPR now formally recognizes the use of BCRs (Article 43). The GDPR also prescribes stricter criteria for the recognition of a country as "adequate," based on the ECJ's decision with regard to the EU-U.S. Safe Harbor Framework (Article 41) (*see also* our 10/06/2015 client alert). Putting in place BCRs entails implementing a comprehensive privacy program which is then subject to the approval of European data protection authorities (DPAs). While each DPA has to approve the BCRs, many DPAs have joined the mutual recognition procedure, meaning that BCRs recognized by one DPA, will be recognized by the others.

**6. Compliance and Governance**

One of the new principles introduced by the GDPR is the accountability principle, which requires that companies must not only comply with the GDPR, but also be able to demonstrate their compliance to regulators on request (Article 22). As part of this effort, companies must have in place a privacy compliance program, document their processing activities, undertake PIAs, implement privacy by design, and in some cases appoint a DPO or even consult with regulators before engaging in certain processing activities.

**Documentation and Recordkeeping.** Currently, in most EU Member States, companies must register their data processing activities with DPAs. The GDPR replaces this requirement with an internal documentation obligation (Article 28). Companies will thus be required to maintain a record detailing, among other things, the purposes of processing; categories of individuals; potential data recipients within and outside the EU; appropriate safeguards for transfers; and security measures. Processors will have similar recordkeeping requirements. Such records must be provided to DPAs upon request. Considering that the documentation requirement applies to all processing, this obligation will likely be quite burdensome.

**Privacy Impact Assessments.** Companies will be required to conduct PIAs for processing activities which are considered likely to result in a "high risk for the rights and freedoms of individuals" (Article 33). These high risk activities will include profiling, large scale use of sensitive data, or systematic monitoring of a public area on a large scale, among others. Furthermore, DPAs will maintain lists of processing activities for which PIAs will be required. The GDPR also lists substantive requirements for the PIA itself, including a systematic description of the processing operations, their purposes, and the interests pursued by the company; an assessment of the necessity and proportionality of the processing; a risk assessment with regard to individual rights; and the safeguards and accountability measures that are envisaged (Article 33(3)). Importantly, if the PIA indicates that processing would result in a high risk (which cannot be mitigated), the company must consult with the DPA. If the DPA is of the opinion that the processing would violate the GDPR, it may issue advice or use its investigatory and enforcement powers (Article 34(3)).

**Privacy by Design and by Default.** The GDPR also introduces an explicit requirement of privacy by design, which requires that companies put in place technical and organizational measures designed to implement data protection principles, such as data minimization, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of individuals (Article 23). The GDPR mentions pseudonymization which means replacing individual identifiers with artificial identifiers (such as replacing a name with an arbitrary number) as an example of such a measure. Other common measures include key coding techniques, limiting access, data minimization, and limiting data retention. Furthermore, the GDPR introduces the requirement that certain measures be enabled by default. For example, companies should implement measures that ensure "that by default personal data are not made accessible without the individual's

intervention to an indefinite number of individuals" (Article 23(2)). This provision seems aimed at preventing personal information from being published on the Internet by default. These new obligations will require that companies consider privacy and data security in their development processes so these measures are built into the product or service from the start rather than being an after-thought.

**Data Privacy Officer.** The GDPR introduces a requirement to appoint a DPO, but only in limited circumstances, such as if the company's core activities require regular and systematic monitoring of individuals on a large scale or if the core activities consist of large-scale processing of sensitive data or data relating to criminal offenses (Article 36). Because of the limited application, it is expected that many companies will not have to appoint a mandatory DPO. The DPO must have expert knowledge of privacy and data protection law and practice, and should be able to perform his/her advisory and monitoring duties and tasks in an "independent manner" (Articles 36, 37, Recital 75). A DPO may be appointed for a group of companies (i.e., the group is not required to have a DPO for each affiliate).

**7. Data Security**

The GDPR requires that companies implement technical and organizational data security measures to ensure a level of security appropriate to the risk involved in the processing. This risk assessment should take into account the likelihood and severity of potential incidents. The GDPR also explicitly mentions certain security measures, including key-coding and encryption, the ability to respond to a physical and technical incident, and a process for ongoing evaluation of the effectiveness of security measures (Article 31).

**Data Breach Notifications.** The GDPR introduces a breach notification duty throughout the EU (Article 31). Companies must notify the competent DPA of a breach within 72 hours after the company becomes aware of it, unless the breach is unlikely to result in a risk for individuals. Companies must also notify the involved individuals of the breach without undue delay, unless the breach is unlikely to result in a *high* risk for individuals. Therefore, if a breach results in no risk for individuals, no notification will be necessary, but if there is some risk to individuals, the DPA must be notified, and if there is a high risk for individuals, both the DPA and individuals must be notified. The duty to notify the DPA about a breach within the required timeframe (72 hours) may become a significant challenge because typical investigations into the nature and scope of the breach will take more time than that allotted period.

**8. Enforcement by Data Protection Authorities**

EU data protection laws are enforced primarily by DPAs as independent agencies with investigatory and fining powers.

**New DPA Powers.** The GDPR provides detailed rules regarding DPAs' tasks and powers. The main innovation is that DPAs are given the explicit power to fine companies found to violate the GDPR. The maximum fine DPAs can impose is EUR 20 million or up to 4% of the total worldwide annual revenue of a company (Article 79). DPAs will now have a lengthy set of tasks including monitoring compliance; promoting awareness; advising governments; providing information to individuals; handling complaints; cooperating with other authorities; conducting investigations; drafting standard contracts for data transfers; drawing up requirements for PIAs; encouraging private codes of conduct and certification mechanisms; and fulfilling any other tasks related to data

protection (Article 52). DPAs have many powers including investigatory powers such as access to equipment and premises and corrective powers such as binding orders and bans on processing, administrative fines, and suspension of cross-border transfers (Article 53). Due to these tasks and powers—especially the high fines—the landscape of data protection enforcement is expected to change considerably.

**9. Conclusion**

The GDPR adds provisions that reflect the digital economy and signify a shift for companies towards a more uniform, yet still rather intricate, legal framework. Although it may take some time before the full implications of the GDPR are understood, companies that want to have a head start should pay particular attention to the topics outlined above. The GDPR applicability regime will further extend data protection requirements to non-EU companies. Stricter limitations on profiling and Big Data may complicate development of, and innovation in, certain business areas. Mandatory data breach notifications to DPAs and individuals will require companies to be ready to act within 72 hours. And all of these new obligations come with unprecedented fines of up to EUR 20 million or 4% of annual worldwide turnover. Other new obligations such as accountability, recordkeeping, and PIAs may require further implementing regulations and DPA guidance before they are actionable.

---

[1] Article numbers refer to the text agreed upon by the EU Council and the EU Parliament in December 2015 and are likely to change when the GDPR is formally adopted.