EU General Data Protection Regulation: What Impact for Businesses Established Outside the EU and EEA

Francoise Gilbert [1]

The EU General Data Protection Regulation (GDPR), which replaces Directive 95/46/EC (Directive), will apply, and enforcement will commence, on May 25, 2018. The repeal of the Directive will take effect as of the date when the GDPR begins to apply.

The GDPR is not just an update of a 20-year old directive that was designed at the dawn of the Internet era, and that was based on privacy principles published by the Organization for Economic Co-operation and Development (OECD) in the early 1980s. It is a significant development in the shaping of the law of privacy and data protection in the European Union as a cohesive, homogeneous whole, where one single law becomes the primary vehicle to govern the activities of very diverse countries in a particular domain.

This article focuses primarily on the obligations faced by companies whose principal business establishment is located outside the European Union (EU) and the European Economic Area (EEA).

Application to Most Companies Worldwide

The most important thing to note about the GDPR is that it is likely to apply to your company, wherever it is located, if it does any business in the EU or EEA, processes personal data of individuals established in the EU, or monitors the activities of European residents. Indeed, the GDPR will apply not only to all entities that are established in the EU/EEA and collect or process personal data in the EU/EEA, but also to a wide range of entities established outside the EU or EEA.

Specifically, the GDPR will apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU/EEA regardless of whether the processing takes place in the EU/EEA or not. In addition, it will apply to the processing of personal data of individuals who reside in the EU/EEA when the processing is conducted by a controller or processor that is not established in the EU/EEA, if such processing relates to: (i) the offering of goods or services in the EU/EEA, whether payment is required or not; or (ii) the monitoring of such individual's behavior, to the extent that such behavior takes place within the EU/EEA. Thus, any website or mobile application that promotes goods or services and is available for access by EU/EEA based individuals – for example, if prices are provided in Euros - is within the scope of the GDPR. Such is also the case of any website or mobile application that contains code that allows the collection of data intended to be used for interest-based advertising.

A partner at Greenberg Traurig, Francoise Gilbert focuses her practice and research on U.S. and global data privacy and cybersecurity in a wide variety of markets, including, among others, Internet, e-commerce, cloud computing, connected devices, sensors, data analytics, artificial intelligence, robotics, and other emerging technologies. She is the author of the two-volume treatise "*Global Privacy and Security Law*," published by Wolters Kluwer (www.globalprivacybook.com), and the co-author of a dozen other books, including "*Internet of Things and Data Analytics*," published by Wiley, and "*Robotic Technologies Law*," published by Larcier. Ms. Gilbert holds CIPP/US, CIPP/EU, and CIPM certifications, and has received law degrees and obtained bar admissions both in the United States and in France.

Improvements

The GDPR attempts in numerous different ways to increase the consistency among the laws and legal regimes of the EU/EEA Member States. This results in particular in reducing several of the obstacles and hurdles that companies used to face. Some of them include the following:

Single Rule … Almost all the Time

The new rule is framed as a "regulation" rather than a directive. That means that it is directly applicable in each of the EU member states and does not need to be transposed into each country's legal framework. The existing EU/EEA data protection framework is based, instead on a series of directives, the main one being Directive 95/46/EC, which are only foundational documents with limited direct application and direct the member states to enact laws that are consistent with the provision of the relevant directive. Given the significant differences between the cultures and legal frameworks of each Member State, the implementation of the 1995 Directive resulted in the creation of national data protection laws that had some resemblance but differed substantially with each other.

The GDPR, as a single document valid throughout the EU/EEA, is intended to bring uniformity; however, despite this appearance of uniformity, it should be noted that numerous provisions give leeway to each member state. Thus, companies must be very careful not to be fooled by the appearance of a single rule, and instead should always consider the general rule as well as the numerous national exceptions or supplements that are likely to be created.

For example, the new provision on the protection of children sets a threshold at age 16, but allows Member States to lower this threshold to age 13 or any number in-between. This is also the case for penalties. While a provision defines the general conditions for imposing administrative fines, another provision allows Member States to lay down the rules for other penalties that would be applicable to infringements of the GDPR that are not subject to the pre-defined administrative fines.

No More Notification … but More Paperwork

Companies that do business in multiple EU/EEA member states frequently complained about the significant administrative burden and related costs that were associated with compliance with the "notification" requirements under the Directive. The notification process requires each company to register its database with the data protection authority of the Member State in which it operates. Registration requirements and registration procedures differ from country to country.

Some countries, such as France, require the completion of a lengthy questionnaire with specific and detailed questions. The response to the questionnaire must be updated each time the company changes its practices. The process is cumbersome and often delays the start of a project.

Other countries, such as the United Kingdom, use a much simpler questionnaire that can be quickly completed. However, the UK requires annual filings, and the payment of a fee at each annual renewal. The GDPR puts an end to the notification requirement. This change could result in significant savings for companies that operate in several Member States.

The GDPR, however, preserves the pre-existing concept of prior consultation or prior authorization, and requires that, in high risk situations, organizations consult in advance with the relevant supervisory authority. It also requires cooperation with the supervisory authorities.

In addition, the GDPR defines a new regime of accountability (discussed below), where companies will have to prepare and maintain numerous documents and reports to record their practices and policies with respect to the handling of personal information, as well as a written information plan to carefully document their information systems and their personal data processing.

One Stop Shop

The One Stop Shop concept is intended to provide companies that operate in several Member States with the ability to deal with one single supervisory authority. Previously, a company that was doing business in several Member States was required to interact with each of the supervisory authorities as applicable because the jurisdiction of these data protection authorities was limited to the Member State where they were established.

With the one-stop-shop structure, if a controller or processor is established in more than one Member State, or if the activities of a single establishment of a controller or processor in the EU substantially affect data subjects in more than one Member State, the supervisory authority of the Member State where the entity has its "main establishment" will act as the lead authority for all data processing activities that have an impact throughout the EU/EEA.

The lead authority may adopt binding decisions, but must coordinate its work with the other supervisory authorities. The GDPR puts in place a complex system of consultation with the other supervisory authorities to ensure that a decision of a lead authority regarding matters that affect several member states takes into account the views of each of the supervisory authorities of the affected member states. In this case, the lead authority is expected to take "utmost account" of the suggestions made by the other supervisory authorities.

The supervisory authority of a member state will continue to have jurisdiction over matters that are limited to that member state. This new structure will have a primary effect on the oversight of multinational companies with offices in several EU countries, but will also help smaller entities.

Transfer of Data Outside the EU

Binding Corporate Rules (BCR) were initially developed by the Article 29 Working Party to allow multinational corporations and groups of companies to make intra-organizational transfers of personal data across borders, as an alternative to Standard Contractual Clauses. With the GDPR, the concept of BCRs receives a boost.

In the current framework shaped under the 1995 Directive, BCRs are recognized only by approximately two-thirds of the Member States. Obtaining approval of BCRs requires a cumbersome process of multiple approvals, which can take 18 to 24 months. Today, less than 100 companies have sought and obtained approval of their BCRs, even though using BCRs as a method to legalize cross-border transfers has been available for approximately 10 years.

The GDPR formally recognizes the BCRs. It creates a consistency mechanism that makes the approval system more efficient and less onerous than the current one. They are available to both data controllers and processors.

The GDPR also expands the number of "appropriate safeguards" that can be used for the transfer of personal data to a third country. In addition to the BCRs discussed above and standard data protection clauses adopted by the Commission (which will replace the three sets of Standard Contractual Clauses currently in existence), it will now be possible to rely on:

- Standard data protection clauses that are adopted by a national supervisory authority and approved by the EU Commission pursuant to an examination procedure defined in the GDPR;
- Approved codes of conduct combined with binding and enforceable commitments of the controller or processor in the recipient country to apply the appropriate safeguards, including with respect to the data subjects' rights;
- Approved certification mechanisms combined with binding and enforceable commitments of the controller or processor in the recipient country to apply the appropriate safeguards, including with respect to the data subjects' rights; and
- Legally binding and enforceable instruments between public authorities or bodies.

Approved Codes of Conduct or Certification Mechanism

The GDPR gives a significant role to codes of conduct and certification mechanisms. Several of the compliance requirements under the GDPR can be addressed by showing adherence to an approved code of conduct, or receiving a certification from an approved organization. For example, the use of approved codes of conduct and approved certification mechanisms, if they are combined with binding and enforceable commitments of the controller or processor in the recipient country to apply the appropriate safeguards, can serve to legitimize the transfer of personal data outside of the EU/EEA.

Challenges

The GDPR also creates new uncertainties and challenges. Some of them are discussed below.

Consent

Where processing of personal data is based on consent, the controller will be required to be able to demonstrate that such consent was given. Under the GDPR, an individual's consent must be given freely, specific, informed, and unambiguous. If an individual gives consent in a written declaration that concerns other matters, the request for consent must be presented in a manner that is clearly distinguishable from other matters, in an intelligent and easily accessible form, using clear and plain language. Otherwise, it will not be binding. Thus, "implied consent" appears to practically be ruled out.

Furthermore, the GDPR will require controllers to allow individuals to withdraw their consent easily and at any time. The GDPR also provides for rules to assess whether consent actually was given freely. For example, consideration will be given to whether the performance of a contract was made conditional on the consent without the relevant data being necessary for such performance.

Without consent, the processing will be deemed lawful only in specific circumstances where the data is processed on a legitimate basis under the GDPR or another law, for example if the data is processed as a necessity for compliance with legal obligations to which the controller is subject, or the necessity for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject before entering into a contract.

The GDPR also addresses the special case of children. For e-commerce, social media, content, or information service providers to process personal data of persons younger than 16 years, the consent of the child's parent or custodian will be required. This is another case where the rule will differ from Member State to Member State. The GDPR allows Member States to lower this age limit to 13 years.

Accountability Obligations

Instead of being required to file notifications with the relevant data protection authorities, organizations will have to be able to demonstrate, in case of an audit by the relevant data supervisory authority, that they have a comprehensive data protection compliance program that meets the requirements defined under the GDPR. For this, they will have to develop, implement, and monitor the application of a series of policies, reports, rules, and contracts that evidence their compliance with the GDPR. Most of these obligations will apply to both data controllers and data processors.

More specifically, among other things, each controller will have to maintain a record of the processing activities under its responsibility. The record will have to include specified information such as the purpose of the processing, the categories of data and data subjects, the categories of recipients to whom the data will be disclosed, including recipients in third countries or international organizations, and the envisaged time limit for the erasure of the different categories of data. Companies will be expected to keep records of transfers of personal data to a third country, and the documentation of the appropriate safeguard to legitimize the transfer, as well.

Other obligations include, for example, keeping a written description of the technical and organizational measures to protect the security of the personal data and an obligation to keep records of activities in order to document the process of selecting data processors and to keep copies of written contract with data processors.

Companies that perform "high risk" activities are subject to additional provisions. The GDPR requires that the entity consult in advance with the applicable supervisory authorities, and conduct a privacy impact assessment.

There are exceptions to the requirements above. For example, enterprises with less than 250 employees will be exempt from most of these requirements unless they operate in high-risk areas or process sensitive data.

Security Breach Notification

The GDPR implements rules regarding the response to a breach of security. A "personal data breach" is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or processed."

The notification of a breach of security will occur in two successive phases.

In case of a personal data breach, the controller is required to notify the competent supervisory authority of such breach "without undue delay" and, if feasible, not later than 72 hours, unless it is unlikely that the breach will result "in a risk to the rights and freedoms of individuals." If the breach is not notified within 72 hours, the subsequent notification must indicate the reasons for the delay. When a breach affects a data processor, it must notify the controller "without undue delay" after becoming aware of the breach.

If the data breach is likely to result in a "high risk to the rights and freedoms of individuals," the controller also will be required to inform the data subjects without undue delay of the occurrence of the breach unless an exception applies. If a data controller fails to notify the affected individuals, the supervisory authority may require the data controller to do so, or may decide that an exception applies.

The GDPR does not define "risk" and "high risk" or provide any guidelines about the difference between the two concepts.

Data Protection Officer

Certain categories of data controllers or data processors will have to appoint a data protection officer. This requirement will apply to all organizations whose core activity consists of the following when they are conducted on a large scale:

- The regular and systematic monitoring of data subjects;
- The processing of special categories of personal data; or
- The processing of data relating to criminal convictions and offences.

Groups of companies will be able to appoint a single data protection officer if that person is easily accessible from each establishment.

It should be noted that this provision of the GDPR may be supplemented by national laws. The GDPR States to supplement the list above to define additional circumstances in which a data controller or data processor would be required to appoint a data protection officer.

Fines

Fines for violations of the basic GDPR principles for data processing (including but not limited to inability to demonstrate that consent was obtained) as well as noncompliance with certain orders of the competent supervisory authority, can be up to the greater of €20 million or 4 percent of the total worldwide annual turnover of

the company for the preceding financial year. For other violations, fines can be up to the greater of 10 million euros or 2 percent of such turnover.

It should be noted that in addition to this general rule, another provision of the GDPR allows Member States to lay down the rules for other penalties that would be applicable to infringements of the GDPR that are not subject to the pre-defined administrative fines.

Next Steps?

Entities that are within the jurisdiction of the GDPR are expected to modify their practices to comply with the new rules defined by the GDPR by May 25, 2018. The task is daunting, for a variety of reasons. Integrating a uniform law within the framework of countries with a diverse culture, diverse personalities, and different levels of friendliness to businesses is by itself a significant hurdle.

Additionally, many of the key concepts in the GDPR are still to be defined. the Article 29 Working Party, the highly respected group comprised of the data protection commissioners of the Member States, is periodically publishing guidelines, such as guidelines on the role of the Data Protection Officer, or the concept of data portability.