wiley

NEWSLETTER

The GDPR's Reach: Material and Territorial Scope Under Articles 2 and 3

May 2017

Practice Areas

Privacy, Cyber & Data Governance

With just over a year to go before the European Union's (EU) General Data Protection Regulation (GDPR or Regulation) comes into force, companies around the world are recognizing the importance of complying with the new laws. According to *Forbes*, analysis from information management company Veritas Technologies suggests that "86 percent of organizations worldwide are concerned that a failure to adhere to GDPR could have a major negative impact on their business" and "nearly 20 percent said they fear that non-compliance could put them out of business."[1] Given that fines under the GDPR can be as high as $21 million or 4 percent of annual turnover, whichever is greater, these fears are hardly baseless.

Nonetheless, confusion reigns over the actual scope of the GDPR, and many non-EU companies are unsure whether they must comply with the new Regulation and, if so, how. That the GDPR will impact many more companies than the EU Data Protection Directive (Directive) it replaces is a dictum. Yet, much of the discussion about the territorial reach of the GDPR appears to be generating more heat than light. While non-EU companies should take EU privacy laws more seriously, there is a risk of taking the fear of non-compliance too far and needlessly chilling innovation. Guidance from regulatory authorities and the Article 29 Working Party will be crucial for understanding the real risk to non-EU companies.

GDPR: A Brief Overview

Adoption of the GDPR – after more than four years of intense debate, negotiation, and lobbying – marked an important milestone in EU data protection laws. The GDPR replaces the EU Data Protection

Directive – a 22-year-old privacy framework. One of the most significant changes in the GDPR is the very fact that it is a "regulation," as opposed to a "directive." A regulation applies directly to EU Member States and, as a formal matter, allows them little discretion in implementation, whereas a directive sets desired results and policies but depends upon Member State implementation into national law. Because regulations automatically become part of each Member State's legal framework, they typically reduce the potential for regulatory patchwork across EU Member States' domestic laws. Whether the GDPR will truly create a consistent data protection framework in the EU remains to be seen – Member States retain the ability to derogate from certain aspects of the Regulation.

The GDPR introduces significant and ambitious changes to EU privacy laws. Under the GDPR, consent must be "freely given, specific, informed, and unambiguous." Data subjects have new rights, including the "right of portability" and the "right of erasure" (also known as the "right to be forgotten"). In addition to broad new rights for data subjects, the GDPR imposes several specific obligations on data controllers and processors, including notice and privacy by design requirements. In some circumstances, data controllers and processors will be required to designate a Data Protection Officer as part of an accountability program. Compared to the Directive, the GDPR also imposes stricter obligations with respect to data breach notifications.

To harmonize application of privacy rules across the EU, the GDPR introduces a "one-stop-shop mechanism" so that businesses with activities in multiple EU countries are primarily subject to the authority of one "lead" data protection authority (DPA). The new Regulation also is backed by a punitive penalty structure that is intended to ensure that data controllers and processors take the protections afforded to data subjects seriously. DPAs have wide-ranging powers to enforce the GDPR, which becomes effective starting May 25, 2018.

Applicability: Does the GDPR Apply to You?

Under the GDPR, jurisdiction is less related to the location where a business is incorporated or headquartered and more to the scope and location of business activity. The GDPR will apply to the processing of personal data by businesses "established" within the EU. More controversially, it also will apply to businesses outside the EU if their data processing activities relate to the offering of goods or services to individuals in the EU or to the monitoring of such individuals' behavior. This latter provision expands the territorial scope of the GDPR well beyond the EU, essentially making it global law.

Material Scope

Article 2 governs the material scope of the GDPR. The GDPR retains much of the jargon from the Directive, although with some important changes. The Regulation applies to the processing of "personal data," which is defined to mean any information relating to an identified or identifiable natural person (a "data subject"). In contrast to the Directive, the GDPR adds special categories of "sensitive data" which include both biometric and genetic data. The GDPR covers all "data processing," which is broadly defined to cover any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. Examples include collection, recording, organization, structuring, storage, adaptation or

alteration, retrieval, consultation, use, disclosure, erasure, or destruction. A person or body (alone or jointly) which determines the purposes and means of processing personal data is a "data controller." An entity which processes data on behalf of the data controller is a "data processor."

Territorial Scope

Article 3 of the GDPR governs its territorial scope. Pursuant to Articles 3(1) and 3(2), the GDPR applies to businesses established in the EU, as well as to businesses based outside the EU that offer goods and services to, or that monitor, individuals in the EU. Article 3(3) adds that the GDPR also applies in places where EU Member State law applies by virtue of public international law. Although each of these provisions provides some contour to the broad scope of the GDPR, they also introduce complexities and gray areas.

1. Article 3(1): "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."

The GDPR applies to businesses "established" in the EU, where personal data is processed "in the context of the activities" of such an establishment. Per the Recitals, establishment "implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect." Once this test is met, the GDPR applies whether the actual data processing takes place in the EU or not.

In this respect, the GDPR is consistent with Article 4(1)(a) of the Directive, which reflects the country of origin concept (i.e., where your business is established dictates which law applies). While this may seem straightforward on the surface, interpretation of Article 4 of the Directive has been beset with complexity. In fact, the Court of Justice of the European Union (CJEU) has struggled with the question of what it means to be "established" and what constitutes processing carried out in the context of the activities of an establishment.

In *Weltimmo v. NAIH* (C-230/14), the CJEU adopted a broad and flexible definition of "establishment" that does not hinge on legal form – indeed, the presence of a single representative may be sufficient. In that case, Weltimmo – which was incorporated in Slovakia – was considered to be established in Hungary by virtue of the use of a website in Hungarian, which advertised Hungarian properties, use of a local agent, and use of a Hungarian postal address and bank account.

Similarly, in *Google Spain SL, Google Inc. v. AEPD, Mario Costeja Gonzalez* (C- 131/12) (known as the "right to be forgotten" decision), the CJEU found that U.S.- incorporated Google Inc. was established in the EU because its search activities were sufficiently linked to the advertising sales generated by Google Spain, a local subsidiary. Because the data processing at issue in that case was related to the search business which Google Spain's sale of online advertising helped finance, the CJEU found that the processing was carried out "in the context of the activities" of the Spanish establishment.

The implications of these decisions are considerable. In both cases, the CJEU found that entities outside the EU could be subject to the Directive – which did not have express extra-territorial reach – because of the activities of a separate operation in an EU Member State. Of course, it is unclear whether these prior interpretations of "establishment" for purposes of the Directive will continue to apply under the GDPR. Indeed, they may be unnecessary given the express extra-territorial authority now granted under Article 3(2).

To the extent these cases continue to apply, the presence in the EU of a branch or subsidiary, or even a single individual, may bring all the data processing activity within the scope of the GDPR. Global businesses will need to show that there is no commercial connection between a local operation and a non-EU company to avoid application of EU data protection laws to data processing by the non-EU company. And unlike the Directive, the GDPR's establishment rule applies both to controllers and processors.

2. Article 3(2): "This regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a. The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

b. The monitoring of their behavior as far as their behavior takes place within the Union."

Unlike the Directive, the GDPR expressly extends the reach of EU data protection laws to businesses based outside the EU. Non- EU established businesses are subject to the GDPR where they process personal data of data subjects in the EU in connection with (i) the offering of goods or services or (ii) monitoring the behavior of individuals in the EU.

Under the first prong, the GDPR explains that having a commerce-oriented website that is accessible to EU residents does not by itself constitute offering goods or services in the EU. Rather, a business must show intent to draw EU customers, for example, by using a local language or currency. Article 3(2) appears to adopt a sliding scale approach as opposed to a bright-line rule, and there is little guidance so far on how to interpret this provision.

However, the CJEU has considered when an activity is "directed at" EU Member States in other contexts. A similar requirement can be found in Article 15 of Regulation 44/2001, known as the Brussels Regulation, which deals with contract disputes involving more than one country. In that context, a joint declaration by the EU Council and the Commission states that "the mere fact that an Internet site is accessible is not sufficient of Article 15 to be applicable, although a factor will be that this Internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance."[2] In *Pammer v. Schulter* (C-585/08), the CJEU found that it was necessary to show that the trader has "manifested its intention to establish commercial relations with consumers from one or more other Member States." To facilitate the application of this test, the CJEU offered a number of criteria to be considered, such as a clear statement by the trader on the website that its goods or services are offered in one or more Member States mentioned by name; the paid inclusion in search engines accessed from particular Member States; or "the international nature of the

activity at issue; ... telephone numbers with the international dialing code; use of a top-level domain name other than that of the Member State ... mention of an international clientele composed of customers domiciled in various Member States."

Based on this guidance, the following factors (among others) may be strong indications that a non-EU business is offering goods or services to data subjects in the EU and may therefore be subject to the GDPR:

- Use of the language of a Member State (if the language is different than the language of the home state);
- Use of the currency of a Member State (if the currency is different than the currency of the home state);
- Use of a top-level domain name of a Member State;
- Mentions of customers based in a Member State; or
- Targeted advertising to consumers in a Member State.

Under the second prong of Article 3(2), businesses monitoring the behavior of individuals in the EU also are subject to the GDPR's requirements. The Recitals specifically contemplate tracking individuals online for purposes of creating profiles, "particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes."

Notably, Article 3(2) applies to the processing of personal data of any individual "in the EU." The individual's nationality or residence is irrelevant. The GDPR protects the personal data of citizens, residents, tourists, and other persons visiting the EU. So long as an individual is in the EU, any personal information of that person collected by any controller or processor who meets the requirements of Article 3(2) is subject to the GDPR. Where Article 3(2) applies, controllers or processors must appoint an EU-based representative.

3. Article 3(3): "This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

The GDPR also applies wherever EU Member State law applies by virtue of public international law. The Recitals provide a single example: a diplomatic mission or consular position. While that case is limited, the rule in public international law established by the Permanent Court of International Justice in Lotus is that a country has any extra-territorial jurisdiction it claims so long as there is not a public international law rule prohibiting the assumption of jurisdiction. Thus, the EU potentially could expand the GDPR scope in the future using this provision.

* * * * *

There is much that still must be clarified about new aspects of EU data protection laws. Guidance from regulatory authorities and the Article 29 Working Party will be crucial for understanding the real scope of Articles 2 and 3. In the meantime, non-EU companies should consider the scope of their activities and their risk tolerance in crafting a GDPR compliance strategy.

[1] Adrian Bridgwater, *Forbes*, "Worldwide Climate of Fear over GDPR Data Compliance Claims Veritas Study" (Apr. 25, 2017) *available at* https://www.forbes.com/sites/adrianbridgwater/2017/04/25/worldwide-climate-of-fear-over-gdpr-data-compliance-claims-veritas-study/#763d37b1680c.

[2] *See* Joint Declaration, Statement on Articles 15 and 73, *available at* http://ec.europa.eu/civiljustice/homepage/homepage_ec_en_declaration.pdf.