Territorial applicability of the GDPR

New EU data protection law also to apply to non-EU organizations

By Sven Schonhofen, LL.M. (New York), and Friederike Detmering, M.A.

On May 25, 2018, the most important reform in EU data protection law in 20 years will enter into force. The General Data Protection Regulation (GDPR) will bring in wide-ranging new obligations. These changes are not only relevant to organizations that are established in the EU, but also to non-EU organizations, which means that all organizations must determine whether the GDPR applies to them.

Where does the GDPR apply?

The GDPR introduces two principles with regard to territorial applicability: establishment and marketplace rule. According to Article 3 of the GDPR, the new regulation applies:

- If the processing of personal data takes place in the context of activities of an establishment of an organization in the EU, regardless of whether the processing takes place in the EU or not ("establishment rule"; Article 3(1) of the GDPR).
- If personal data of individuals who are in the EU is processed by an organization not established in the EU and the processing concerns
  - the offering of goods or services to individuals in the EU or
  - monitoring the behavior of individuals that takes place in the EU ("marketplace rule"; Article 3(2) GDPR).

Practical advice

Organizations with more than one establishment in the EU may benefit from the one-stop-shop principle regarding the competency of supervisory authorities (Article 56 of the GDPR). For this purpose, they must determine their main establishment, which is the place of central administration in the EU.
What is the establishment principle?

The GDPR applies to organizations that process personal data in the context of an establishment in the EU (Article 3[1] of the GDPR). An establishment requires the effective and real exercise of activity through stable arrangements. The concept of establishment is flexible and not formalistic, so one representative of an organization may suffice.

The processing must take place in the framework of the activities of an establishment. The establishment, however, does not need to carry out the processing itself. Further, it is irrelevant whether the processing activities are carried out within or outside the EU. Organizations established in the EU, therefore, cannot avoid the applicability of the GDPR merely by processing personal data outside the EU.

The marketplace rule in the GDPR

In contrast to the Data Protection Directive (DPD) adopted in 1995, Article 3(2) GDPR features a marketplace rule that also covers internet-related questions if goods and services are offered to individuals in the Union online.

Whose personal data are covered by the marketplace rule?

The marketplace rule requires the processing of personal data of individuals who are in the Union. The applicability of GDPR in this respect is tied to the physical presence of an individual in the Union (even temporarily), irrespective of the individual’s nationality, residence or intention to stay within the EU (recital 14 to the GDPR). An individual “who is in the Union” can be an EU citizen or a citizen of a non-EU country, such as a tourist, cross-border commuter, expatriate, refugee or stateless person.

When do organizations offer goods and services to individuals in the Union?

The GDPR applies under Article 3(2) if goods and services are offered to individuals in the Union. The offering does not need to be connected to payment. Goods or services offered for free are also included.

The marketplace rule focuses on offering and not performing. The GDPR does not apply where US users are addressed (services are offered) and the user travels to the EU during the performance of an agreement. This does not fall under the marketplace rule as the actual marketplace would be in the US and not the EU.

Behavior monitoring does not have to be aimed at individuals in the EU, but the monitored behavior must take place in the Union.

What is the monitoring of behavior?

The GDPR also applies if the organization monitors the behavior of users in the EU. Behavior monitoring refers to techniques for tracking individuals’ internet activities, such as profiling and targeting in the context of advertising (e.g., via cookies), location monitoring in mobile apps or monitoring via wearables.

Practical advice

Organizations seeking to bypass the applicability of the marketplace rule must avoid giving the impression that they offer goods or services to users in the EU. This can be accomplished by:

- not offering to provide services to EU users on websites/in marketing materials
- removing all EU countries in address fields or similar drop-down menus
- not allowing users located in the EU to sign up for services
- not offering shipments to the EU or payment in EU currencies
- including disclaimers on the landing page of the organization’s website stating that neither services nor goods are intended to be offered to users from the EU
- not entering into direct contractual relationships with EU end customers

Moreover, the language of the GDPR focuses on offering and not performing. The GDPR does not apply where US users are addressed (services are offered) and the user travels to the EU during the performance of an agreement. This does not fall under the marketplace rule as the actual marketplace would be in the US and not the EU.
in the Union. The GDPR is thus not applicable if an EU citizen is monitored during a stay in the US.

The lack of a requirement to explicitly address EU individuals constitutes a very broad applicability of the GDPR as any website operator who uses tracking or profiling measures must comply with the GDPR requirements.

**Consequences: Representative and one-stop-shop principle**

If Article 3(2) of the GDPR is applicable, organizations not established in the Union have to designate in writing a representative in the Union in accordance with Article 27 GDPR.

If the GDPR is applicable pursuant to Article 3(2) of the GDPR, the organization does not have an establishment in the EU. The organization therefore does not benefit from the GDPR’s one-stop-shop principle as it is not possible to define a lead supervisory authority.

**Conclusion and to-dos**

Organizations located inside and outside the EU should carefully determine whether they must abide by the rules of the GDPR and should monitor the upcoming guidance from the Article 29 Working Party on Article 3 of the GDPR. They must also determine if national GDPR implementation laws apply (please see Reed Smith local law chart for details).

There is not long left to prepare for the GDPR and organizations should focus on topics that have high priority for supervisory authorities:

- reviewing the current status of processing activities and maintaining a record of processing activities
- having clear internal privacy responsibility structures (e.g., appointing data protection officers)
- implementing procedures for handling individual rights and being transparent
- ensuring data security, in particular having a data-breach policy in place
- determining a lead supervisory authority

---

**Practical advice**

In order to avoid being subject to the GDPR due to internet-related monitoring activities, organizations should consider:

- Not dropping analytics cookies with EU IP addresses
- Geoblocking website users from the EU (some supervisory authorities have indicated that this might not be sufficient, though)

---

**Editor's note:**

Please see also Reed Smith LLP Technology Law Dispatch Blog (tw)