The European Data Protection Board issues long-awaited guidelines on the territorial scope of the GDPR

Data Protection, Privacy and Security Alert

30 NOV 2018
By: Carol A. F. Umhoefer | Lea Lurquin

This week the European Data Protection Board (EDPB) issued for public comment its Guidelines on the territorial scope of the European Union General Data Protection Regulation (GDPR). One of the purposes of GDPR was to expand the application of EU data protection law, but the provisions setting out GDPR's scope are not consistently clear.

Approximately one year in the making, the Guidelines confirm some of the established interpretations of GDPR's application to entities in the EU even when they process personal data of persons outside the EU and clarify GDPR's scope particularly as to the meaning of "persons in the Union." The Guidelines also discuss the conditions when a non-EU entity subject to GDPR must designate a representative in the EU.

Still, the Guidelines leave unanswered important questions, including whether non-EU entities offering B2B services or goods to EU companies fall under GDPR.

In November 2017, the then-Article 29 Working Party group of EU data protection supervisory authorities – now the EDPB – was tasked with providing guidelines on the interpretation of GDPR Art. 3, which sets out the scope of

application of GDPR to entities established in the EU (Art. 3(1)) and entities established outside the EU (Art. 3(2)).

Application of GDPR to entities "established" in the EU

Art. 3(1) states that GDPR 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 Guidelines follow the well-established doctrine of the Court of Justice of the European Union in the *Costeja* ("right to be forgotten") and *Weltimmo* cases, rendered in 2014 and 2015, respectively: a controller or processor of personal data will be considered to have an establishment in the EU if it exercises in the territory of a member state a real and effective activity (even if minimal) through stable arrangements, regardless of its legal form (eg, subsidiary, branch, office). The Guidelines state that the presence of a single employee or even a sales representative in the EU may suffice to create an establishment in the EU, provided that such employee or sales representative acts with a sufficient degree of stability.

The Guidelines also refer to the "inextricably linked" test formulated in the *Costeja* case – if the processing activities of a non-EU entity are inextricably linked to the activities of an establishment in the EU, GDPR will apply whether or not the EU establishment is taking any role in processing personal data.

For non-EU entities, the Guidelines clarify several key issues that arise under Art. 3(1), and in particular state that a non-EU entity will not be deemed to be established:

- Solely by virtue of merely using a data processor located in the EU
- Merely because its website is accessible from the EU or
- By virtue of having designated a representative in the EU because it is subject to GDPR under Art. 3(2).

Application of GDPR to entities that are not "established" in the EU

Art. 3(2) states that GDPR 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."

In what is sure to be an important clarification, the Guidelines state that persons "in the Union" are persons who are *located* in the EU when they are targeted with an offer of goods or services or by the monitoring of their behavior. Nationality, residence or legal status of the individual is irrelevant.

In other words, GDPR is not intended to extend to all EU citizens wherever they may be, but instead protects the data of persons in the EU, including persons who are temporarily in the EU such as tourists, *if* while in the EU they are targeted with offers of goods or services, or targeted in order to monitor their behavior.

The Guidelines also reiterate numerous criteria drawn from existing case law as to when a non-EU entity can be considered to target a person in the EU with an offer of goods or services, such as the language of the offer, the currency for payment or references to customers who are in the EU.

Regarding monitoring, the Guidelines confirm that "monitoring" is not limited to online tracking but includes CCTV and other offline activities such as monitoring of health status. The Guidelines also posit that all online collection or analysis of personal data of persons in the EU does not automatically count as monitoring. Instead, it is necessary to consider the purpose for processing the data and in particular any subsequent behavioral analysis involving that data.

On this point, the Guidelines adhere closely to GDPR recital 24, which describes monitoring as the tracking "of persons on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

The Guidelines therefore clarify several key issues that arise under Art. 3(2) for non-EU entities:

- Services targeted at persons who are transient in the EU – such as tourists – will fall under GDPR. The Guidelines provide as an illustration an application, offered by a US startup without any EU establishment, that offers city mapping and targeted advertising for tourists, including London, Paris and Rome maps.
- If goods or services are not targeted to persons in the EU, then GDPR will not apply. For example, when a US tourist vacationing in Europe downloads a US news app targeting US residents, the personal data collected will not be subject to GDPR.
- The data of EU citizens is not automatically covered by GDPR. If a Taiwanese bank active only in Taiwan processes personal data of German customers residing in Taiwan, that data will not be subject to GDPR.

Designating an EU representative

Art. 27 requires controllers and processors established outside the EU, but subject to GDPR pursuant to Art. 3(2), to designate a representative that is established in an EU member state where individuals whose personal data is processed are located. The Guidelines advise that if a significant proportion of those individuals are located in one member state, it is good practice to designate a representative located in that member state.

The Guidelines reiterate GDPR requirements for controllers to designate the representative in writing; for controllers to include in their privacy notice the identity and contact details of the representative; for representatives to maintain (with the help of the controller or processor) the Art. 30 record of processing activities; and per Recital 80, for the representative to be subject to enforcement proceedings in the event of the controller or processor's non-compliance.

The Guidelines also provide helpful practical advice:

- The representative may be a natural or legal person; if the latter, a lead contact should be appointed.
- The representative's mandate may be part of a service contract.
- A representative may act on behalf of several non-EU controllers and processors.
- A representative may not act as an external DPO of the controller or processor.
- Similarly, a processor may not be appointed as EU representative of its customer-controller.
- The representative may rely on a team to communicate in the local language of individuals and supervisory authorities.

Finally, the Guidelines reiterate the exemptions to designating a representative, namely, if the processing is occasional, does not include large scale processing of special categories of data or criminal convictions and offenses data and is unlikely to result in a risk to individuals' rights and freedoms. Unfortunately, the Guidelines do not clarify the meaning of "occasional."

The questions the Guidelines don't answer

A number of questions remain unanswered, however.

- One of the most critical open issues is whether GDPR applies when an individual in the EU is targeted solely in a professional capacity and only for the purpose of offering goods or services to that individual's employer. Many US entities without any EU establishment are in exactly this position.
- Another question is how to determine when logging or tracking (such as counting subscribers' usage) crosses the line and becomes behavioral analysis and therefore "monitoring" under Art. 3(2).
- Yet another question is how to determine when processing is "related to" an offer of goods or services, or monitoring of behavior. The Guidelines state that there must be a connection to the offer or the monitoring, and that such connection may be direct or indirect, but do not offer any further specifics.
- For US entities using EU processors, the Guidelines make clear that the processors are subject to GDPR, including the transfer requirements in Chapter V, implying that the transfer of a US customer's data from the EU back to the US needs to be made pursuant to Privacy Shield or a derogation, given that the Standard Contractual Clauses do not cover transfers from EU processors.
- Finally, the Guidelines do not discuss exceedingly common scenarios that arguably create an EU establishment under Art. 3(1), such as when a US parent company processes data of its EU subsidiaries' employees in connection with calculating yearly bonuses, setting up training programs or fixing annual objectives.

The EDPB is accepting comments from all interested stakeholders and citizens on the draft Guidelines until January 18, 2019. Learn more about the Guidelines and their implications for you by contacting either of the authors.

AUTHORS

Carol A. F. Umhoefer
Partner
Miami | T: +1 305 423 8500
carol.umhoefer@dlapiper.com

Lea Lurquin
Associate
San Francisco | T: +1 415 836 2500
lea.lurquin@dlapiper.com