Jan 2020

EU: EDPB guidelines on the territorial scope of the GDPR

On 12 November 2019, the European Data Protection Board ('EDPB') adopted the final version of its guidelines ('the Guidelines') on the territorial scope of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') almost one year after the guidelines had been published in draft form[1]. Wim Nauwelaerts, Partner at Alston & Bird, provides a summary of the Guidelines and highlights areas where additional guidance may be needed going forward.

mf-guddyx / Signature collection / istockphoto.com

Scope

A key question, and one that is often neglected, is whether the GDPR actually applies to a specific data processing activity, particularly if the controller or processor involved in that processing is located outside of the EU. Since the GDPR came into force, the provisions on territorial application in Article 3 of the GDPR have given rise to different interpretations among privacy professionals, as well as supervisory authorities. This has led to confusion as to when the GDPR should apply if there is a 'non-EU' dimension to a data processing activity, for instance, because the controller responsible for the data processing has no physical presence in the EU, but uses a processor in the EU to process personal data on its behalf. Realising the need for urgent guidance on this topic, the EDPB adopted draft guidelines on 16 November 2018, which were submitted for a two-month public consultation. The EDPB then published its Guidelines having taken account of the contributions and feedback that it received from various stakeholders. In addition to providing guidance on the application of Article 3 of the GDPR, the Guidelines address the requirements for non-EU controllers or processors, subject to the GDPR, to designate a representative in the EU, which is set out in Article 27[2].

Two main criteria

The territorial scope of the GDPR is determined on the basis of two main criteria: the 'establishment' criterion in Article 3(1), and the 'targeting' criterion in Article 3(2). If either of these criteria is met, the relevant provisions of the GDPR will apply to the data processing, and subsequently the controller and/or processor involved in that data processing, will have to ensure compliance with those provisions. However, the Guidelines emphasise that certain processing activities may fall within the ambit of the GDPR, while other processing of personal data by the same controller or processor may not[3]. Therefore, it is important to undertake a careful assessment of a controller's or processor's different processing activities in order to determine which ones are in the scope of the GDPR.

The establishment criterion

As per Article 3(1), the GDPR applies to the processing by a controller or processor carried out in the context of the activities of an establishment of that controller or processor in the EU. Whether or not the actual processing takes place in the EU is irrelevant. The Guidelines recommend analysing the different elements of this criterion before concluding whether or not the GDPR applies.

Establishment in the EU

The concept of 'establishment' of the controller or processor in the EU is interpreted broadly and refers to any real and effective activity, even a minimal one, in an EU Member State, and is exercised through stable arrangements, regardless of the legal form. To determine if a controller or processor has an establishment in the EU, both the degree of stability of the local arrangement, as well as the effective exercise of a business activity in one or more EU Member States, should be taken into account. It is not necessary to have an affiliate, subsidiary, or branch in the EU in order to be established for the purposes of Article 3(1), and according to the Guidelines, the mere presence of one employee in the EU may trigger the application of the GDPR, even if the controller or processor is actually based outside of the EU[4]. In that case, however, it must be clear that the processing of personal data by the controller/processor outside of the EU is carried out in the context of the activities of the EU-based employee. Also, the fact that a company's website is accessible by individuals in the EU does not by itself suffice to conclude that the company is established in the EU, and therefore within the scope of the GDPR.

Processing in the context of the activities of the establishment in the EU

The GDPR applies if personal data are being processed in the context of the activities of an establishment of the controller or processor in the EU, irrespective of whether or not that establishment is involved in carrying out the processing. To determine if this condition is fulfilled, the Guidelines recommend conducting a case-by-case analysis of the facts[5]. If that analysis demonstrates that there is an inextricable link between the data processing of a controller or processor outside of the EU, and the activities of that controller/processor's establishment in the EU, the GDPR will apply to the non-EU controller or processor. An EU establishment generating revenues in the EU can be indicative of processing that is carried out in the context of the activities of a non-EU controller or processor, if the underlying business activity is inextricably linked to the processing of personal data outside of the EU. The Guidelines provide the example of an e-commerce website operated by a China-based company, which has an office in Germany focusing on commercial prospects and marketing campaigns in the EU[6]. The EDPB considers that the activities of the German office are inextricably linked to the processing of personal data carried out by the Chinese e-commerce website, insofar as the commercial prospecting and marketing campaigns towards EU individuals serve to make the e-commerce business of the Chinese company profitable. The Chinese company's processing of personal data can therefore be viewed as being carried out in the context of the activities of the German office, as an establishment in the EU. Therefore, the data processing will be subject to the GDPR, as per its Article 3(1).

Regardless of where the processing takes place

The GDPR applies to processing of personal data in the context of the activities of an establishment in the EU, regardless of where the processing takes place. It is not relevant whether the actual processing takes place in the EU or outside of the EU. The Guidelines provide the example of a Sweden-based pharmaceutical company that has located all processing activities relating to clinical trial data in its branch based in Singapore[7]. In this case, although the data processing takes place in Singapore, it is considered to be carried out in the context of the activities of the pharmaceutical company, for example, the controller/sponsor of the clinical trials established in Sweden. The GDPR therefore applies to this specific data processing pursuant to Article 3(1).

Regardless of the location or nationality of the data subjects

The Guidelines make it clear that Article 3(1) does not restrict the application of the GDPR to the processing of personal data of individuals who are in the EU or have EU citizenship[8]. Any personal data processing in the context of the activities of an establishment of a controller or processor in the EU may fall within the scope of the GDPR, regardless of the location or the nationality of the data subjects whose personal data are being processed. This clarification, which is supported by Recital 14 of the GDPR, is helpful because in the past there has been considerable confusion on this topic, leading some controllers and processors with an establishment in the EU to believe that they had to protect the personal data of EU nationals or EU residents only.

The GDPR does not automatically apply to both a controller and processor

If both controllers and processors are involved in a data processing activity, the application of the establishment criterion must be assessed for each controller and processor separately. In the opinion of the EDPB, a processor in the EU should not be considered to be an establishment of a controller, outside of the EU, within the meaning of Article 3(1), merely because of its processor status. Put differently, the existence of a relationship between a controller and a processor does not necessarily trigger the application of the GDPR to both.

If a controller meets the establishment criterion and uses a processor established in the EU, both will be subject to their respective obligations under the GDPR. If, on the other hand, a controller meets the establishment criterion and uses a processor without an establishment in the EU, the Guidelines explain that the controller will need to ensure that it puts in place a contract with the processor addressing all the requirements that EU-based processors have to comply with, which is set out in Article 28(3) of the GDPR[9]. The processor located outside the EU will, therefore, become indirectly subject to GDPR obligations, which are contractually imposed by the controller subject to the GDPR. In addition, if the processor is based in a country outside of the EU for which there is not adequacy finding, the data transfer restrictions in Chapter V of the GDPR will need to be considered. These may require the controller and processor to put in place, for instance, controller-to-processor Standard Contractual Clauses ('SCCs').

Less straightforward are the scenarios in which a controller does not meet the establishment criterion and uses a processor established in the EU. If the processor is processing personal data on behalf of the non-EU controller in the context of its establishment in the EU, it will be subject to GDPR processor obligations under Article 3(1). However, this does not mean that the non-EU controller is automatically subject to the GDPR controller obligations, simply because it chooses to use a processor in the EU. The EDPB takes the view that by instructing a processor in the EU, a controller outside the EU is not carrying out processing in the context of the activities of the processor in the EU[10]. However, even though the controller is not in scope of the GDPR, the EU-based processor will be subject to the relevant processor obligations in the GDPR. According to the Guidelines, these include the provisions on transfers of personal data to third countries or international organisations, as per Chapter V of the GDPR. Unfortunately, the Guidelines do not explain or provide practical examples of how processors should comply with the GDPR's data transfer restrictions in this case. This is particularly problematic as processors cannot use the current versions of the SCCs, one of the most popular mechanisms for transferring personal data outside of the EU, as 'data exporters.' This may prompt processors to rely one of the transfer 'derogations' in Article 49 of the GDPR, but traditionally their use has been heavily restricted by the supervisory authorities. Further guidance from the EDPB in this regard would be more than welcome.

The targeting criterion

Even if a data processing activity does not meet the establishment criterion in Article 3(1), the GDPR can still apply if the targeting criterion in Article 3(2) is met. Per Article 3(2), the GDPR applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:

- the offering of goods or services, irrespective of any payment, to data subjects in the EU; or
- the monitoring of their behavior, as far as their behaviour takes place within the EU.

The application of the 'targeting criterion,' as per Article 3(2), can therefore be triggered by two different activities, namely the offering of goods/services, or behavioral monitoring towards data subjects in the EU.

Offering of goods/services

The first activity triggering the targeting criterion in Article 3(2) of the GDPR is the 'offering of goods or services' to data subjects in the EU, irrespective of whether payment is made in exchange for the goods or services provided. The targeting criterion can only be met if there is a clear intention on the part of the controller outside of the EU to offer goods or services to individual data subjects located in the EU. To establish whether a controller has such intention, the EDPB suggests assessing a combination of various factors, including reference to an EU address or phone number on an offering document, and the use of a language or currency of one or more EU Member States[11]. However, the EDPB recalls that when goods or services are inadvertently or incidentally provided to an individual in the EU, the related processing of personal data will not fall within the territorial scope of the GDPR. The Guidelines refer to the example of a university in Switzerland that launches a Master degree selection process and uses an online platform where candidates can upload their CV[12]. The selection process is open to any student with a Bachelor degree and the university does not specifically advertise to students at EU-based universities. Without other factors to indicate the specific targeting of students in EU Member States, it cannot be established that the processing in question relates to the offer of an education service to data subjects in the EU, and therefore such processing will not be subject to the GDPR.

Monitoring of behaviour

The second type of activity triggering the targeting criterion in Article 3(2) is the monitoring of data subject behaviour, provided that such behaviour takes place within the EU. Compared to the offering of goods or services, this criterion is arguably more difficult to apply in practice and the guidance on this specific point was therefore eagerly anticipated. According to the Guidelines, behavioural monitoring for purposes of Article 3(2)(b) of the GDPR encompasses a broad range of activities that involve tracking of individuals on the internet or through other types of networks or technologies. Examples provided by the EDPB include behavioural advertisement, online tracking through the use of cookies, and monitoring or regular reporting on an individual's health status, for example, via wearables[13]. However, the EDPB does not consider that any online collection or analysis of personal data of individuals in the EU automatically amounts to behavioural monitoring. The controller outside the EU must have a specific purpose in mind for the collection and subsequent reuse of data about an individual's behaviour within the EU. Contrary to the situation where a controller outside the EU is offering goods or services, the Guidelines provide that the controller does not need to have the 'intention to target' individuals in the EU in order for Article 3(2)(b) to apply. In other words, the Guidelines appear to suggest that in order for Article 3(2)(b) to apply, the data processing must serve a specific purpose of behavioural analysis or profiling, but it is not necessary that the controller intends to target individuals in the EU. This begs the question, if intent to target plays no role, why is behavioural monitoring covered by the targeting criterion?

Data subjects in the EU

The Guidelines stress that the application of the targeting criterion is not limited by the citizenship, residence, or other type of legal status of the data subjects whose personal data are being processed[14]. However, in order for the targeting criterion to apply, the data subjects must be located in the EU. The requirement that data subjects are located in the EU must be assessed at the time of the relevant trigger activity, for example, when goods or services are being offered or individuals' behaviour is being monitored. The EDPB further notes that, if the processing relates to a service that targets data subjects outside the EU and that is not withdrawn when these data subjects enter the EU, for instance, for travel purposes, the related processing will not be subject to the GDPR.

The Guidelines also clarify that the processing of personal data relating to a data subject in the EU is not sufficient to trigger the application of the GDPR to processing activities of a controller or processor not established in the EU. There also needs to be an element of 'targeting' individuals in the EU, either by offering goods or services to them or by monitoring their behaviour[15]. The EDPB has therefore busted the myth that the GDPR would apply to a company or organisation outside of the EU by the mere fact that it holds personal data about individuals in the EU.

When both the controller and processor are outside of the EU

Complex issues may arise when the targeting criterion in Article 3(2) applies and the controller outside the EU uses a processor that is also not established in the EU to process personal data relating to individuals in the EU on behalf of the controller. In the Guidelines, the EDPB has added a separate section that aims to address these issues[16]. The EDPB takes the position that when a processor is not established in the EU, in order to determine whether its processing may be subject to the GDPR as per Article 3(2), it is necessary to look at whether the processing activities by the processor 'are related' to the targeting activities of the controller. The Guidelines further specify that any processor outside of the EU instructed to carry out data processing related to the targeting activities of the controller will fall within the GDPR's scope, with regard to that processing. Take, for instance, a cloud service provider outside the EU that engages in data processing activities relating to targeting of individuals in the EU by its customer, and therefore a controller established outside of the EU. According to the Guidelines, the processing activity by the cloud service provider/processor on behalf of its controller is likely to fall within the scope of the GDPR, as per Article 3(2) of the GDPR.

Concluding remarks

The Guidelines provide useful clarifications, particularly for controllers and processors outside the EU who have been in doubt as to whether or not the EU data protection rules apply to them. They largely reaffirm prior interpretations of the GDPR's establishment criterion under Article (3)(1), and offer essential guidance with respect to the GDPR's heavily debated extraterritorial application under Article (3)(2). A missing piece in the Guidelines is the interplay between the application of the territorial scope of the GDPR, as per Article 3, and the provisions on international data transfers, as per Chapter V of the GDPR. Further regulatory guidance on this interplay is considered essential, as conventional data transfer mechanisms such as SCCs are not always suitable, for example, in cases where a processor in the EU needs to transfer personal data outside of the EU, and the controller is not established in the EU. It remains to be seen if and when the EDPB will issue such additional guidance. In the meantime, controllers and processors that are in scope of the GDPR by virtue of the establishment or targeting criteria would be well-advised to carefully assess how to comply with the GDPR's data transfer restrictions.

Wim Nauwelaerts Partner
wim.nauwelaerts@alston.com
Alston & Bird, Brussels

---

1. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
2. Pages 23-28 of the Guidelines.

3. Page 5 of the Guidelines.
4. Page 6 of the Guidelines.
5. Page 7 of the Guidelines.
6. Page 8 of the Guidelines.
7. Page 9 of the Guidelines.
8. Page 10 of the Guidelines.
9. Page 11 of the Guidelines.
10. Page 12 of the Guidelines.
11. Page 18 of the Guidelines.
12. Page 19 of the Guidelines.
13. Page 20 of the Guidelines.
14. Page 14 of the Guidelines.
15. Page 15 of the Guidelines.
16. Pages 20-22 of the Guidelines.

RELATED CONTENT

NEWS POST

USA: FTC issues blog post on improved data security orders

MEDIA

Mridula Mutharaju, Head of Privacy & Records Management at NatWest Markets

NEWS POST

EU: EDPS publishes preliminary opinion on data protection and scientific research

NEWS POST

Iceland: Persónuvernd issues decision on unlawful email marketing

OPINION

EU: EDPS comments on facial recognition technology