GDPR Update: EDPB Guidelines on the territorial scope of the GDPR

December 19, 2018

Introduction

On November 16, 2018, the European Data Protection Board (the EDPB) issued draft guidelines on the GDPR's territorial scope. The guidelines are now subject to public consultation, which means they may still be amended. For an introductory explanation on the GDPR's territorial scope, we refer to one of our earlier GDPR updates. This update builds on that update and summarizes the ways in which the EDPB guidelines further clarify the criteria to determine the application of the GDPR's territorial scope.

Furthermore, we address the non-EU organizations' obligation to designate a representative in the EU; the practical issues organizations face as a consequence of this obligation; and the risks of failing to appoint such representative.

The territorial scope of the GDPR

The territorial scope of the GDPR is determined by Article 3 GDPR. The GDPR's territorial applicability is determined by three criteria. If one of the three criteria is met, the GDPR applies from a territorial perspective. The EDPB's findings with regard to these criteria are summarized below.

The GDPR applies to:

i. The processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU (regardless of whether the processing takes place in the EU).
   - An important take-away from the EDPB guidelines in this regard is that the existence of a relationship between a controller and a processor does not necessarily trigger the application of the GDPR to both, should only one of these two entities have an establishment in the EU. The applicability of the GDPR depends on the location of the establishment of the controller or the processor itself.

   - The EDPB considers that when an EU based processor processes personal data on behalf of a non-EU controller, the processor does not qualify as an establishment of the non-EU controller within the meaning of article 3(1) GDPR solely by virtue of its processor status. The EDPB sets out that by instructing a processor in the EU, the non-EU controller is not carrying out processing "in the context of the activities of the processor in the EU." The processing is carried out in the context of the controllers' own activities; the processor is merely providing a processing service which is not "inextricably linked" to the activities of the controller. In such a case, the non-EU controller will therefore not fall under the scope of article 3(1) GDPR, solely because it contracted an EU based processor.

     The processor, in such a case, will be subject to the GDPR by virtue of article 3(1) GDPR, as it is processing

data in the context of its own establishment in the EU. As a consequence, the processor will have to comply with the GDPR processor obligations, including entering into a processing agreement with the controller (article 28 GDPR) and maintaining a record of processing activities (article 30 (2) GDPR).

- The EDPB further considers that a non-EU processor that is not subject to the GDPR, does not become subject to the GDPR only because it processes personal data on behalf of a controller in the EU. It will of course be necessary for the controller to ensure that the processing is governed by a GDPR compliant processing agreement. In practice, this means that the processor will (indirectly) become subject to a number of GDPR obligations. A breach of these GDPR obligations by the processor will qualify as a breach of contract vis-à-vis the controller and not as a direct breach of the GDPR.

ii. The processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, when the processing relates to the offering of goods or services.

- Processing activities relating to the offering of goods and services fall within the GDPR's territorial scope. The EDPB considers that there needs to be a connection between the processing activity and the offering of goods and services, but both direct and indirect connections are relevant. The EDPB does not elaborate on this and does not provide examples of such related processing activities, which raises uncertainties with regard to the exact scope of article 3(2)(a) GDPR.

- To assess whether an organization offers services or goods directed at data subjects in the EU, all relevant facts of the case should be taken into account. In its guidelines, the EDPB provides a non-exhaustive list of nine factors that could play a role in this assessment. These factors are:
    - The EU or at least one EU member state is designated by name with reference to the good or service offered.
    - The marketing and advertisement campaigns are directed at EU member states; or the organization pays a search engine operator for an internet referencing service to facilitate access to its site in the EU.
    - The activity at issue has an international nature (e.g. tourist activities).
    - The mention of dedicated contact details is to be reached from an EU member state.
    - There is a use of EU top-level domain names (e.g. ".nl" or ".eu").
    - The description of travel instructions are from one or more EU member states to the place where the service is provided.
    - There is mention of an international clientele composed of customers domiciled in EU member states.
    - A language or currency of one or more EU member states is used.
    - Delivery of goods is offered in an EU member state.

- The EDPB stresses that several of the factors set out above, if taken alone, may not amount to a clear indication of an organization's offering of goods or services in the EU. However, they should each be taken into account to assess whether the combination of factors qualifies as the offering of goods and services directed at data subjects in the EU.

iii. 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 monitoring of their behavior.

- Recital 24 GDPR appears to limit the concept of monitoring exclusively to the monitoring of behavior through the

tracking of a person on the internet. Whether the EDPB would subscribe to this restrictive interpretation of article 3(2)(b) GDPR, which does not include other types of behavior monitoring (for example through wearables or smart devices), remained an open question. In its guidelines, the EDPB now clarifies that it considers that tracking through other types of networks or technology should also be taken into account in determining whether a processing activity can be qualified as "monitoring behavior." The EDPB is therefore of the opinion that recital 24 GDPR does not limit the scope of article 3(2)(b) GDPR. The EDPB mentions the following examples of monitoring behavior that should be taken into account as well:

  - Behavioral advertisement
  - Geo-localization activities, in particular for marketing purposes
  - Online tracking through the use of cookies of other tracking techniques such as fingerprinting
  - Personalized diet and health analytics services online
  - CCTV
  - Market surveys and other behavioral studies based on individual profiles
  - Monitoring or regular reporting on an individual's health status

- As opposed to article 3(2)(a) GDPR, neither article 3(2)(b) GDPR, nor its guiding recital 24 GDPR introduce a necessary degree of 'intention to target' on the part of the organization to determine if the monitoring activity would trigger the application of the GDPR to its processing activities. The EDPB takes the view that article 3(2)(b) GDPR requires that the organization must have a specific purpose in mind (i.e. an intention) for the collection and subsequent reuse of the personal data about an individual's behavior within the EU. In this regard, the EDPB does not consider that any online collection or analysis of personal data of individuals in the EU would automatically count as "monitoring."

Worth noting is that the EDPB sets out that criteria (ii) and (iii) above, both require an "intention" of the organization performing the processing activities. The EDPB interprets "intention" as having a certain purpose in mind for the collection and further processing of the personal data. As the party determining the purposes and means for the processing, this "intention" is typically something a controller would have. Typically, a processor would not have an own intention to process the personal data; it processes personal data on behalf of a controller. Taking this into account, one could question whether a non-EU processor can fall within the scope of article 3(2) GDPR. The EDPB does not address this particular point, and its examples are all processing activities by controllers.

Interim conclusion

The EDPB emphasizes that, as a general principle, where the processing of personal data by a controller or a processor falls within the territorial scope of the GDPR, all provisions of the GDPR apply to the processing. Non-compliance with the GDPR will expose organizations to significant fines and liability, and, more importantly, possible reputational damages. Hence, we recommend that organizations offering goods and services internationally undertake a territorial scope assessment to determine whether the related processing of personal data falls under the scope of the GDPR.

The representative

According to article 27 of the GDPR, if a non-EU controller or processor falls under the GDPR by virtue of article 3(2)

GDPR (see (ii) and (iii) above), that organization is obliged to appoint a representative within the EU by written mandate. The representative may be a natural or legal person and must be located in one of the EU member states where the data subjects whose personal data are processed are located.

Only when the processing is “occasional, does not include, on a large scale, processing of special categories of data or criminal data” and “is unlikely to result in a risk to the rights and freedoms of natural persons” is the non-EU controller not obliged to appoint a representative. Clearly, these are exemptions, meaning that in practice in most of the cases non-EU organizations covered by the GDPR will be required to appoint a representative.

Public authorities and bodies are exempted from the obligation to appoint a representative.

The EDPB does not consider the role of representative compatible with the role of the DPO. The GDPR requires that the DPO does not receive any instructions regarding the exercise of his or her tasks. The EDPB states that this requirement of independency cannot be reconciled with the role of representative in the EU, as the representative is subject to a mandate from the controller or processor.

The representative is responsible for facilitating the communication between the data subjects and the organization represented, to make the exercise of data subjects’ rights effective. Furthermore, the representative is the main contact for the EU data protection supervisory authorities. Efficient communication with the data subjects and the supervisory authorities requires that the representative (with the help of a team if necessary) is able to communicate in the languages of the parties concerned.

In addition to the abovementioned tasks, the representative must maintain a record of processing activities under the responsibility of the controller or the processor. The EDPB is of the view that the maintenance of this register is a jomint obligation: the organization represented must provide the representative with accurate, complete and up-to-date information so that the record can be maintained and made available by the representative.

In practice, it is our experience that organizations are having difficulties finding parties that are willing to act as representative. One of the reasons for this could be that supervisory authorities can initiate enforcement actions against representatives in the same way as against controllers or processors. The EDPB stresses that this includes the possibility to impose administrative fines and penalties, and to hold representatives liable.

As far as we are aware, at this moment, there is only a limited number of organizations offering external representative services, and as a consequence of the actions that can be initiated against such organizations, costs for the services are significant.

Practical guidance from the EDPB for organizations having difficulties with appointing a representative would have been useful. Instead, in its guidelines, the EDPB emphasizes that failing to appoint a representative constitutes a breach of the GDPR, and thus exposure to significant fines and liability. However, obvious questions remain regarding the likelihood that any enforcement action taken against organizations without a physical presence in the EU would be successful.

Please click here to subscribe to our monthly updates on the GDPR.

Overview of subjects

January 2017	Territorial scope of the GDPR
February 2017	The Concept of Consent
March 2017	Sensitive Data
April 2017	Accountability, Privacy by Design and Privacy by Default

May 2017	Rights of Data Subjects (information notices)
June 2017	Rights of Data Subjects (access, rectification and portability
July 2017	Rights of Data Subjects (erasure, restriction, objectand automated individual decision-making)
August 2017	Data Processors
September 2017	Data Breaches and Notifications
October 2017	Data Protection Officers
November 2017	Transfer of Personal Data (outside the EEA)
December 2017	Regulators (competence, tasks and powers)
January 2018	One Stop Shop
February 2018	Sanctions
March 2018	Processing of Personal Data in the Employment Context
April 2018	Profiling and Retail
May 2018	Overview
October 2018	Overview of developments since May 25, 2018
November 2018	Data Protection Impact Assessments (DPIAs)
December 2018	EDPB Guidelines on the territorial scope of the GDPR

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com

Celine van Es
Associate, Amsterdam
D +31 20 795 31 22
M +31 6 11 16 30 45
celine.vanes@dentons.com