
PUBLISHED: November 29, 2018
AUTHORS: David W. Powell, Kevin L. Walsh

Recently, the European Data Protection Board (EDPB), the body composed of the representatives of the European national data protection authorities, issued draft guidelines on how the General Data Protection Regulations (GDPR) for the European Union (EU) (and more broadly, the European Economic Area or EEA) apply to activities outside of Europe. Extraterritorial application, particularly in the area of employee benefits, has been a hot topic under these regulations, which generally became effective on May 25, 2018. A particular focus has been on the imposition under GDPR of numerous requirements of a new nature, such as a requirement of consent by the data subject to certain uses of data, the “right to be forgotten” (i.e., data deleted), and a requirement that data be kept no longer than necessary. Potential penalties for violations can be substantial.

The EDPB indicates in their new draft guidelines their intention to establish, in terms of data protection requirements, a level playing field for companies active on the EU markets in a context of worldwide data flows. In these particular draft guidelines, the EDPB addresses the territorial scope of GDPR and sheds light on a number of issues in that area. It should be kept in mind that the draft guidelines are only a draft, and the EDPB has requested comments by January 18, 2019, and so may be subject to change.
This article will briefly survey the new draft guidelines, which are fairly complex, and so are likely to be subject to more study and interpretation, as well as possible revision. The guidelines generally apply to controllers and processors of data, terms which generally mean those persons determining the purposes and means of the processing of personal data, and those processing personal data on behalf of the controller, respectively. The guidelines essentially have four parts-

- Application where the controller or processor of data is in the EU;
- Application where neither the controller or processor is in the EU;
- Processing in places where EU law applies by virtue of public international law (which will not be discussed in this memorandum); and
- Appointment of data privacy representatives in the EU by controllers or processors subject to GDPR but not having an establishment in the EU.

US plan sponsors and benefit plans may wish to jump to Part II, the discussion of when neither the controller or processor has an establishment in the EU - an area where the draft guidelines suggest the application of GDPR may be narrow - but would be advised to begin with the discussion of when an establishment in the EU exists, because the guidelines appear to apply GDPR in this area fairly broadly, and may require contractual extension of GDPR to entities outside the EU that would not otherwise be subject to the rules.

I. Application of GDPR Where an Establishment Exists in the EU – Art. 3(1) of GDPR

Article 3(1) of the GDPR provides that the 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 EU, regardless of whether the processing takes place in the Union or not.

What is an “establishment” in the EU?

Here the guidelines indicate that an establishment implies “the effective and real exercise of activities 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.”

The guidelines provide that, in some circumstances (at least in online activities), the presence of one single employee or agent of the non-EU entity may be sufficient to constitute a stable arrangement. Although the notion of establishment is broad, however, it is not without limits, and the guidelines also indicate that it is not possible to conclude that the non-EU entity has an establishment in the EU merely because the undertaking’s website is accessible in the EU.
What is processing of personal data carried out “in the contest of the activities of” an establishment?

The guidelines indicate that there must be some connection between the processing of the data and the activities of the establishment in the EU. This is not to be interpreted restrictively; the guidelines indicate that the existence of some commercial activity led by a non-EU entity within a Member State may be so far removed from the processing of personal data by the entity that the existence of the commercial activity in the EU would not be sufficient to bring that data processing within the scope of GDPR. Non-EU organizations are recommended to identify potential links between the activity for which the data is being processed and the activities of any presence of the organization in the EU.

Need to contractually extend GDPR protections outside of the EU when the controller or processor is established in the EU

As noted above, just because a processor is located outside the EU and may not itself have an establishment inside the EU is not the end of the inquiry. The proposed guidelines go on to state that GDPR is not restricted “to the processing of personal data of individuals who are in the Union…. personal data processing in the context of the activities of an establishment of a controller or processor in the Union would fall under the scope of the GDPR, regardless of the location or the nationality of the data subject whose personal data are being processed.” [emphasis added]

Further, the guidelines state that “the controller may need to consider imposing, by contract, the obligations placed by the GDPR on processors subject to it. That is to say, the controller would have [to] ensure that the processor not subject to the GDPR complies with the obligations, governed by a contract or other legal act under Union or Member State law, referred to Article 28(3) [i.e., the requirements for a processor subject to GDPR]. The processor not subject to the GDPR will therefore become indirectly subject to some obligations imposed by controllers subject to the GDPR by virtue of contractual arrangements.” [emphasis added]

An example in the guidelines explains how broadly this may apply:

A Finnish research institute conducts research regarding the Sami people. The institute launches a project that only concerns Sami people in Russia. For this project the institute uses a processor based in Canada. While the GDPR would not formally apply directly to the Canadian processor, the Finnish controller has a duty to only use processors that provide sufficient guarantees to implement appropriate measures in such manner that processing will meet the requirement of the GDPR and ensure the protection of data subjects’ rights. The Finnish controller needs to enter into a data processing agreement with the Canadian processor, and the processor’s duties will be stipulated in that legal act.

Thus, under these guidelines, processors of personal data outside the EU, and not otherwise subject to GDPR, may expect to be requested to contractually agree to apply GDPR to data provided by controllers within the EU - even if the data subjects are not within the EU.
II.  Application of GDPR Where Neither the Controller nor Processor has an Establishment in the EU – Art. 3(2) of GDPR

The absence of an establishment in the EU does not necessarily mean that a data controller or processor established in a third country such as the US would be excluded from the scope of the GDPR. Art. 3(2) of 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 whether a payment of the data subject is required, to such data subjects in the EU; or
- The monitoring of their behaviour as far as their behaviour takes place within the EU.

The guidelines indicate that the requirement that the data subject be located in the EU must be assessed at the moment when the relevant trigger activity takes place, i.e. at the moment of offering of goods or services or the moment when the behaviour is being monitored.

Moreover, the guidelines also provide that the fact of processing personal data of an individual in the EU alone is not sufficient to trigger the application of the GDPR to processing activities of a controller or processor not established in the EU. The element of "targeting" individuals in the EU, either by offering goods or services to them or by monitoring their behaviour must always also be present.

A helpful example is provided:

A U.S. citizen is travelling through Europe during his holidays. While in Europe, he downloads and uses a news app that is offered by a U.S. company. The app is exclusively directed at the U.S. market. The collection of the U.S. tourist’s personal data via the app by the U.S. company is not subject to the GDPR.

Thus, temporary presence of a data subject in the EU may not be enough to extend GDPR to a data processor in the US – provided that the activity for which the data is being processed is exclusively directed at the US market.

Another area discussed in the guidelines is what offering of goods or services in the EU means. Notably, the guidelines provide an example which may apply to many US benefit plan service providers:

A private company based in Monaco processes personal data of its employees for the purposes of salary payment. A large number of the company’s employees are French and Italian residents. In this case, while the processing carried out by the company relates to data subjects in France and Italy, it does not take place in the context of an offer of goods or services. Indeed human resources management, including salary payment by a third-country company cannot be considered as an offer of service within the meaning of Art 3(2)a. The processing at stake does not relate to the offer of goods or services to data subjects in the Union (nor to the monitoring of behaviour) and, as a consequence, is not subject to the provisions of the GDPR, as per Article 3. [emphasis added]
Monitoring of data subjects in the EU

Although it can probably be fairly said that the provisions of GDPR directed at online monitoring are more aimed at e-commerce, the guidelines provide some indication that health monitoring of persons in the EU may also be subject to the rules.

For example, the guidelines provide that GDPR may apply where a data controller or processor monitors the behaviour of data subjects who are in the EU under a broad range of monitoring activities, including in particular personalized diet and health analytics services online, and monitoring or regular reporting on an individual’s health status.

III. Appointment of EU Representative for Controllers or Processor Not Established in the EU

Even if a controller or processor of personal data does not have an establishment in the EU, if they are subject to GDPR (such as by offering of goods and services to data subjects in the EU, or monitoring their behaviour), the controller or processor may be required to appoint a representative in the EU to perform or act on its behalf with regard to the entities GDPR obligations. This obligation may be fulfilled through a service contract with a third party that provides such services. There are also certain exemptions from this requirement, where, for example, processing is occasional and does not include large scale processing of certain data, and such processing is unlikely to result in a risk to the rights and freedoms of natural persons.

IV. Conclusion

At first blush, the proposed territorial scope guidelines are helpful to US data processors and controllers in some regards, but may be less helpful in others. The potential impact of GDPR on US benefit plan sponsors and the plans themselves is worth considering, particularly in light of the potential of contractual obligations to data controllers or processors that have an establishment in the EU. As these guidelines are finalized and digested, this will be an area where monitoring is advisable.

If you have any questions about these guidelines, or are interested in submitting comments to the EDPB, please contact David Powell, Kevin Walsh, or your regular Groom lawyer.