

Publications

New Guidance on the Territorial Scope of GDPR Impacts U.S. Benefit Plans

ATTORNEYS & PROFESSIONALS

Kelly A. Geloneckkgeloneck@groom.com

202-861-5418

Kalena Ketteringkkettering@groom.com

202-861-0157

David Levinedlevine@groom.com

202-861-5436

George Sepsakosgsepsakos@groom.com

202-861-0182

PUBLISHED

11/21/2019

SOURCE

Groom Benefits Brief

SERVICES

Employers & Sponsors

- Retirement Programs
- Fiduciary & Plan Governance
- Health & Welfare Programs

Health Services

- Privacy & Security
- Plan Services & Providers

Retirement Services

On November 12, 2019, the European Data Protection Board (“EDPB”) released final guidelines on the territorial scope of the European Union’s (“E.U.”) General Data Privacy Regulation (“GDPR”). These guidelines come nearly a year after the release of the initial version published for public consultation. Given the global marketplace, participants in United States (“U.S.”) employee benefit plans may be located in the E.U., thus raising concerns about the GDPR’s applicability to U.S. plans. As a result, plan sponsors and service providers have been concerned that travelling or expatriate participants, or U.S. employees seconded to an EU subsidiary for some time, could cause them to become a “processor” (or possibly a “controller”) of plan related data and therefore to become subject to GDPR. For example, if a participant checks their 401k balance or files a claim electronically while on vacation or living in the E.U., would that act trigger GDPR?

The newly released final guidelines address some of the territorial scope questions plans have been asking and that were discussed our recent GDPR related alerts:

<https://www.groom.com/resources/chaotic-rollout-for-european-data-privacy-regulations-raises-questions-for-benefit-plan-administrators/> and <https://www.groom.com/resources/prepare-for-territorial-scope-guidance-under-gdpr/>

Article 3 of GDPR establishes its territorial reach. Under Article 3, an entity’s activity is subject to GDPR if it: (1) has an “establishment” in the E.U.; or (2) is “targeting” individuals in the E.U. As most U.S. based benefit plans do not have a permanent establishment in the E.U. (though their plan sponsors might), the “targeting” criterion has received the most attention in the U.S. benefits space.

The EDPB stresses that “targeting” activity must be ascertained on a case-by-case basis. The guidelines outline a two-step approach to determining if processing activity constitutes targeting: (1) the processing must relate to the personal data of individuals who are in the E.U.; and (2) the processing must relate either to the (a)

offering of goods or services, or (b) the monitoring of those individuals' behavior in the E.U. We expand upon each element of the test below.

Individuals in the European Union

The EDPB explains that GDPR seeks to protect everyone in the E.U. regardless of whether or not they are citizens of the E.U. The guidance, however, clarifies that in relation to the offering of goods and services, the “targeting” provision is only aimed at activities that intentionally, as opposed to incidentally, target individuals in the E.U. Thus, if processing relates to a service only offered to individuals outside the E.U. but the service continues when individuals enter the E.U., that processing is generally not subject to the GDPR. In this case, the processors are targeting individuals outside the E.U., but not withdrawing services when the individual no longer remains outside the E.U.

The guidelines provide an example of an Australian subscriber of an Australian company's mobile phone service traveling to Germany. The Australian company targets their service exclusively to Australian users with Australian phone numbers. However, a user travels to Germany and continues to use the service. The example says that although the Australian subscriber is using the service in Germany, the company has not “targeted” users in the E.U., so the Australian company is outside the scope of the GDPR.

In contrast, the guidelines provide a counterexample of a U.S. app company that creates a tourist application for individuals to use while in Europe. The U.S. company processes users' information to send advertisements of nearby European restaurants. The example says that the U.S. company would be considered to be “targeting” individuals in the E.U., so the U.S. company would be subject to the GDPR. In another example, where a Chinese company had an office in the E.U., the processing of personal data related to E.U. sales was subject to GDPR.

Offering of Goods or Services and Monitoring Behavior

EDPB explains that the provision “offering of good or services” applies to processors regardless of whether the good or service requires payment. As an example, the guidelines explain a U.S. company processing travel reimbursements of employees on a temporary business trip to Europe would not constitute an offer of services to those individuals because such processes constitute human resource obligations and are not an offer of a good or service. Whether the same answer would apply if processing benefits for a person seconded to work at an E.U. subsidiary or branch for a longer period is not directly addressed. As the final guidelines note, the mere presence of an employee in the E.U. is not as such sufficient to trigger the application of the GDPR, because for the processing in question to fall within the scope of the GDPR, it must also be carried out in the context of the activities of the EU-based employee. Thus, the specific activities of the EU-based employees may be relevant.

In another example, employees work in Monaco (not an E.U. country) but reside in France (which is an E.U. country). The example says that even though the employees are E.U. citizens, processing salary information is not the same as offering goods or services. The example goes on to say that “human resource management” is not considered as an offer of a service or relate to monitoring under GDPR.

Additionally, EDPB notes that any collection or analysis of personal data of individuals located in the E.U. would not automatically constitute “monitoring behavior.” Instead, it is necessary to consider the purpose of collecting the data and the subsequent analysis. The applicability of the monitoring provision is broad, and the EDPB explains it could encompass: behavioral advertising, geo-locating activities (especially for marketing purposes), online tracking, personalized online health analytic services, CCTV, market surveys, or regular reporting of health status.

An example is given of a U.S. company that developed a health and lifestyle app, allowing users to record with the U.S. company their personal indicators (sleep time, weight, blood pressure, heartbeat, etc.). The app provide users with daily advice on food and sport recommendations. The processing is carried out by the U.S. data controller. However, the app is made available to, and is used by, individuals in the E.U. For the purpose of data storage, the U.S. company uses a processor established in the U.S. (cloud service provider). In this case, to the extent that the U.S. company is monitoring the behavior of (“targeting”) individuals in the E.U., both the activity of the controller and the processor are within the scope of the GDPR.

Information Obtained from Entities with Establishments in the EU

Note, too, that where a U.S. plan as a data processor receives personal data from a controller in the E.U., it may be asked to agree to GDPR-like contractual protections by the E.U. controller. 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 Union, regardless of the actual place of the processing.

GDPR does not provide a definition of “establishment” for the purpose of being subject to GDPR. The final guidelines state, though, that the legal form of such arrangements, whether through a branch or a subsidiary, is not the determining factor in that respect. Rather, the E.U. courts have ruled that the notion of establishment extends to any real and effective activity — even a minimal one — exercised through stable arrangements. As a result, in some circumstances, the presence of one single employee or agent of a non-E.U. entity in the Union may be sufficient to constitute an establishment. Thus, it may be necessary to determine whether U.S. controllers (or processors) have any establishment in the E.U. to which the data relates.

Some commercial activity carried out by a non-E.U. entity within the E.U. may, however, 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 the data processing by the non-E.U. entity within the scope of GDPR.

The final guidelines go on to state, though, that where a controller with an establishment in the E.U. chooses to use a processor located outside the E.U. for a given processing activity, it will be necessary for the controller to ensure by contract or other legal act that the processor processes the data in accordance with the GDPR.

Summary and Next Steps

While the guidelines aim to clarify the GDPR’s territorial scope and suggests that U.S. retirement plans, may often be outside GDPR’s scope, it will be important to monitor E.U. courts and guidance from country regulators as they further interpret GDPR’s scope. Benefit plans may need to conduct a closer review of the types of information gathered about enrollees and how that information is processed to determine whether activities give rise to “monitoring” when providing services to individuals who are in the E.U. The specific activities of employees in the E.U. may also be relevant, as well as whether the U.S. data controller or processor has an establishment in the EU to which the data relates. Further, to the extent that additional E.U.-focused services are offered to participants in a health or retirement plan, increased diligence to determine whether GDPR compliance obligations are triggered may be warranted.

If you have any questions about how GDPR may apply to your plan or business, please contact your regular Groom attorney or any of the attorneys listed here.

[New Guidance on the Territorial Scope of GDPR Impacts U.S. Benefit Plans](#)[Download](#)