

Publications

Chaotic Rollout for European Data Privacy Regulations Raises Questions for Benefit Plan Administrators

ATTORNEYS & PROFESSIONALS

Kevin L. Walshkwalth@groom.com

202-861-6645

PUBLISHED

06/14/2018

SOURCE

Groom Benefits Brief

SERVICES

[Employers & Sponsors](#)

- [Fiduciary & Plan Governance](#)

[Retirement Services](#)

- [Plan Services & Providers](#)

On Friday, May 25, 2018, the European Union's General Data Privacy Regulation ("GDPR") took effect. As a result, you have likely received a flood of consent requests in your email inbox and you may have noticed some of the chaos that has resulted. For example, within hours complaints were filed against Facebook and Google seeking in excess of nine billion Euros for alleged breaches, many U.S. newspapers blocked European IP addresses from accessing their websites, and some churches in England have ceased praying for the sick by name out of fear that that could run afoul of GDPR restrictions on health data. The situation has been best summed up by U.S. Secretary of Commerce Wilbur Ross who stated that, "GDPR creates serious, unclear legal obligations for ... private sector entities ... [and] we do not have a clear understanding of what is required to comply." As a result, the U.S. government has already requested that European regulators act quickly to provide "clearer rules".

For U.S. benefit plan administrators and service providers, GDPR is daunting because of its scope, vagueness, and enforcement mechanism that includes fines of up to 20 million Euros or four percent of worldwide turnover. While GDPR is designed to protect the privacy rights of individuals and was largely crafted in response to concerns about the types and volume of information being gathered by technology companies (and certain governments), it applies to all companies that are considered "controllers" or "processors" of information of natural persons who are located in the European Union. Currently, there is no short term exception, and GDPR defines "personal data" as essentially any information relating to a data subject, even name and email address (though with more rules for certain data such as that related to health).

At bottom, this means that GDPR's obligations could be triggered not only if a plan covers a European resident but, if applied literally, also if information is processed while a U.S. participant is travelling in the European Union (examples could include if

the plan gathers the IP address information of individuals who access the plan's website, if a participant's address is updated, or if the participant accesses health benefit services while in Europe).

The possibility that the European Union could interpret GDPR as applying in these situations and the fear of fines has led to two primary questions. First, what are data controllers and data processors? And second, how does each comply? We note that GDPR is in its early stages and, based on the disruptive rollout, it is clear that no entity can currently be certain that it is in compliance without additional clarification from European regulators.

We will try to briefly summarize the duties of data controllers and data processors.

Data Controller

What is a "data controller"? A data controller is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" of natural persons in the European Union. Under GDPR, data controllers are viewed as the entities that have the primary compliance obligations as they are the entities that decide what data to collect and how to use it.

To comply with GDPR, a data controller needs to

1. Conduct an information audit;
2. Determine a legal basis to process data;
3. Establish adequate safeguards for cross-border data transfers;
4. Provide privacy notices to data subjects;
5. Establish infrastructure to implement data subject rights; and
6. Implement data breach processes.

At its core, controllers are required to ensure that there is a legal basis for all gathering and processing of data. This includes minimizing the data gathered, protecting data, disclosing what data is being gathered and how it is being used, and recognizing the rights that individuals have to control data (which may include rights to know exactly what data is being collected and to request its deletion). Two areas that seem to be generating the most concern are that the data subject give affirmative consent to the use of his or her data, and to have it deleted, subject to exceptions, and that data be kept no longer than necessary.

As the entity with the primary compliance responsibility, controllers are responsible for the actions of the data processors that they use. "Where processing is to be carried out on behalf entities of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject." Essentially, this means that controllers will want to draft strict contracts with processors and obtain robust indemnification against misuse of data on EU persons – assuming processors will be willing to accept the responsibility.

In the employee benefit plan context, a plan fiduciary or service provider is likely a controller or processor if it has any information about who the plan's participants are, even if only by name. However, obtaining consent from participants may not always be necessary as GDPR permits some data gathering and processing if an entity has a legitimate interest in the data subject's personal data. In the plan context, the legitimate interest could be complying with legal requirements to provide benefits. This could cover the gathering of sufficient information to identify an individual, determine benefits, and locate the individual to provide the benefits due. This is only an exception to the consent requirement, though, not to all of GDPR, and one point of caution is that European regulators may narrowly construe what information and processing is "necessary" for the provision of benefits. Another concern is how to determine when data is no longer need and must be deleted.

Data Processor

A "data processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." "Processing" is defined as carrying out any operation on the data, including collection, recording, storage, consultation or use. Unlike a controller, a processor is an entity that has no discretion over the use of data and gathers and molds it based on the

instructions from a controller. Note that, as a result, whether an entity is merely a data process or is also functionally a data controller may not be clear, particularly where the processor has some discretion over plan administration.

GDPR imposes a number of requirements on processors such as:

1. Only processing on instructions from the controller;
2. Obtaining consent before using a subcontractor;
3. Returning or deleting personal data at the end of service contracts;
4. Allowing audits by the controller;
5. Securing the data;
6. Notifying the controller of data breaches;
7. Limiting transfer of data to other countries and international organizations; and
8. Maintaining records.

For the most part, the obligations of processors will, at least in theory, be set out in the contracts they enter into with controllers. Here, we note that those contracts will contain provisions prohibiting the use of information for any purpose other than those that the processor is ordered to use the data for. And processors not only risk violating the GDPR obligations on processors by using data outside the scope of their contracts but also risk becoming controllers if data is used for other purposes. For personal data that is provided by EU controllers to US processors, national legislation under GDPR provides certain rules for EU controllers providing data to entities outside the EU, but the application of those laws in the context of US benefit plans is still in the early stages.

Conclusion

For now, plans and service providers should be paying attention to GDPR. Some basic steps that could be taken to comply include determining whether the plan covers any individuals who are located in the European Union, determining whether the plan possesses any data that it does not need to provide benefits, and possibly blocking European IP addresses from accessing plan websites without consent (as a way of signaling that some efforts have been taken to comply). US benefit plan data controllers and processors may begin to see GDPR-related privacy agreement requests from EU entities. At the same time, full compliance is likely far away. GDPR is vague and compliance even among European data companies is far from complete, despite extraordinary amounts of money being spent in the effort.

US plans sponsors and recordkeepers may wish to reach out to regulators to seek clearer guidelines for US employee plans covering EU individuals. In the interim, it is a subject to closely monitor.

If you have any questions, please contact the authors or your regular Groom lawyer.

[Chaotic Rollout for European Data Privacy Regulations Raises Questions for Benefit Plan Administrators](#)[Download](#)