GROOM LAW GROUP CHARTERED

BENEFITS BRIEF

May 11, 2016 www.groom.com

Authors: David W. Powell, Kevin L. Walsh

If you have questions, please contact your regular Groom attorney or one of the attorneys listed below:

George M. Gerstein
ggerstein@groom.com
(202) 861-6650

Richard K. Matta
rmatta@groom.com
(202) 861-5431

Louis T. Mazawey
lmazawey@groom.com
(202) 861-6608

David W. Powell
dpowell@groom.com
(202) 861-6600

Kevin L. Walsh
kwalsh@groom.com
(202) 861-6645

New EU Data Privacy Regulation May Impact US Benefit Plan Administrators

On May 4, 2016, the European Parliament and European Counsel published Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "Data Privacy Regulation"). This long-awaited Data Privacy Regulation may impact US pension and benefit plan administrators working with plans that cover European Union (EU) citizens or individuals (which may include US citizens) residing within the EU. This is because the Data Privacy Regulation applies to the "processing" of personal data not only where the "controller" or "processor" is in the EU, but also where a non-EU "controller" or "processor" is processing personal data of individuals in the EU and the processing is related to the offering of goods or services to EU residents or the monitoring of their behavior. (It is unclear whether the Data Privacy Regulation might apply to plans that cover EU citizens who do not reside within the EU, and that possibility raises some concern. This is an area where further guidance may be useful.) The Data Privacy Regulation takes effect on May 25, 2018 and will apply to non-EU countries in the European Economic Area (EEA) as well.

"Processing" of personal data is broadly defined to mean any operation or set of operations which are performed on personal data including: collection, recording, organization, structuring, storage, adaption, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"Personal data" is also broadly defined to mean any information relating to an identified or identifiable natural person, such as a name, an identification number, location data, an online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

The impact on US plan administrators appears to arise in two circumstances. First, US plan administrators may need to comply with the Data Privacy Regulation if the plan administrator gathers, processes, or has another entity gather or process personal data of individuals in the EU and it is determined that the processing is related to the offering of goods or services to EU residents. It appears that processing data in connection with the offering of pension or welfare benefits to EU residents could be deemed to be in connection with the offering of services. Because personal data includes national identification numbers and health information, it appears likely that administrators of both pension and welfare plans will be deemed to gather or process some personal data if any plan participant or beneficiary resides in the EU. The second circumstance where the Data Privacy Regulation may impact plan administrators is where they seek access to data that has been gathered by an EU company. Under the Data Privacy Regulation, EU companies can only share personal data in limited circumstances such as (1) with entities based in countries that the European

Commission concludes have sufficient personal data privacy regulations, or (2) companies that agree contractually to terms similar to the Data Privacy Regulation. Presumably, the Commission will be developing further guidance on the adequacy of personal data protection in non-EU jurisdictions such as the US.

If a US plan administrator needs to comply with the Data Privacy Regulation for the first reason outlined above, it is likely that the plan administrator will be required to appoint in writing a representative in the EU. This representative appears to be for the purpose of facilitating the ability of EU regulators to oversee the use of the data and investigate and penalize a non-EU entity. A representative will generally be needed unless the processing is occasional, does not include, on a large scale, processing of special categories of data, and is unlikely to result in a risk to the rights or freedoms of natural persons, taking into account the nature, context, scope, and purposes of the processing. It may be difficult to conclude that a plan administrator meets this exception.

Under the Data Privacy Regulation, personal data must be (1) used fairly, (2) collected for specified, explicit, and legitimate purposes, (3) gathered only to the extent necessary, (4) accurate and kept up to date, (5) kept in a form that permits identification no longer than is necessary, and (6) protected. Health data and certain other special categories of data have a higher standard for processing. Additionally, individuals have strong rights to correct inaccurate data, request that data be deleted, and to limit use of data.

Additionally, the Data Privacy Regulation details policies and procedures that need to be in place when data is used, how it can be used, how it should be saved, and the notices that need to be provided when personal data is gathered. Plan administrators may need to develop procedures to the extent a plan administrator becomes subject to the rule.

Finally, the Data Privacy Regulation has significant sanctions. A person who has suffered "material or non-material damage" as a result of infringement of the Data Privacy Regulation has a right to damages. European regulators can impose fines of up to the greater of 20 million euros or 4% of total worldwide annual turnover of the preceding financial year.

Plan sponsors in the US may wish to begin considering how the new Data Privacy Regulation may apply to their plans, and, fortunately, have some time to do so.