DAVIS GILBERT

Employers Beware: New EU Data Law May Impact Employee Benefits

The Bottom Line

- GDPR is already in effect and fines could be levied for non-compliance.
- U.S. based employers should work with their legal counsel to review their plan participant population to determine whether GDPR applies and to ensure that GDPR's requirements are satisfied.

May 25, 2018 was the compliance enforcement deadline for the EU's General Data Protection Regulation (GDPR), which governs the collection, use and storage of private information of EU residents. U.S.-based companies should not assume that GDPR does not apply to their U.S.-based benefit plans. The fact is, a company (or its plan) does not have to be located in the EU to be subject to GDPR requirements.

Another common misconception among U.S.-based companies is that plans subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) already have sufficient data protections in place so that compliance with HIPAA satisfies compliance with GDPR. In actuality, GDPR's data security requirements differ from HIPAA. Moreover, California recently adopted a law, the California Consumer Privacy Act of 2018, based on GDPR that will go into effect in 2020, and it is possible that other states will follow suit. Thus, U.S.-based companies would be wise to consider GDPR's potential impact on their benefit plans now.

A number of open questions remain as to the applicability of GDPR, including:

1. Is it applicable to U.S. based retirement plans in cases where retirees have relocated to the EU?
2. Is it applicable to offshore data processing?
3. Is it applicable if a U.S. resident is travelling in the EU and accesses plan information while travelling?

These are critical considerations given that violations of GDPR can result in fines of up to four percent of annual worldwide gross revenue or €20 million (whichever is greater). Employers should review their plans and related service provider contracts to determine if any changes are necessary in light of GDPR.

This alert summarizes key aspects of GDPR and lays out steps that plan sponsors should take to ensure compliance.

GDPR Summary

GDPR was adopted in 2016 to replace the 1995 Data Protection Directive. It regulates how companies process and protect the personal data of all individuals situated within the EU. Key data protection components of GDPR include:

- Having a legal basis for the processing of personal data
- Maintaining appropriate categories of records on data processing activities

- Providing data subjects with increased rights concerning the use and disclosure of their data
- Increasing transparency in data processing practices of companies
- Giving regulators more power to investigate breaches and impose penalties

GDPR also gives member states authority to pass laws to supplement GDPR, which will result in additional compliance requirements and variations in local processing practices. GDPR not only impacts companies in all industries and jurisdictions, but it can impact various departments within companies, including human resources and benefits.

Next Steps for Plan Sponsors

Employers should review their employee and retiree populations to determine whether any employees and/or retirees are residing in the EU, regardless of citizenship, which would necessitate a more in-depth review. Employers should also consider taking the following steps:

- Review all third-party provider services to identify where personal data is shared with third parties. If personal data is shared, review all applicable service provider agreements to determine whether amendments are necessary.
- Consider what data is collected and whether collection of that data is necessary.
- If consent is requested from employees or retirees, ensure that GDPR's consent requirements are satisfied and determine whether consent is the best legal basis to accomplish data processing goals.
- Review all privacy notices provided to plan participants and revise as necessary to comply with GDPR.
- Review all data security and breach notification processes. GDPR requires notification of data breaches to individuals without undue delay (excluding certain limited exceptions).
- Provide privacy training. Companies should already be providing HIPAA privacy training, but the scope of the training should expand to cover GDPR issues as well. GDPR may also require training employees who would not need to be trained under HIPAA.

Related People

Mark E. Bokert
Partner/Co-Chair
212 468 4969
mbokert@dglaw.com

Alan Hahn
Partner/Co-Chair
212 468 4832
ahahn@dglaw.com

Gabrielle White
Counsel
212 468 4962
gwhite@dglaw.com