One Employee in Europe Could Trigger New EU Data Protection Obligations

Dana B. Rosenfeld

May 16, 2017

An Update on the New EU General Data Protection Regulation

On 16 April 2016, the EU adopted the General Data Protection Regulation ('GDPR') which largely rewrites and harmonizes the European legal framework of data protection. The new regulation will become applicable in May 2018, but given the scope and complexity of the GDPR it is important to prepare for this legal change well in advance.

Global scope?

With the GDPR, there will be a substantial expansion of the territorial scope of the EU data protection obligations, which may impact US companies and employers who were previously not affected by EU data protection rules. In determining its geographical reach, the GDPR considers not only the location of the processing, but also the location of the individual whose data is being processed. In this context, if your group of companies has one EU-based employee, the GDPR could be applicable to your organization. Note that the GDPR would also be triggered by processing personal data of EU-based customers.

Processing information?

If your group of companies has one EU-based employee, and it *processes* (i.e., collect, use, transfer or electronically store) personal data of this employee the GDPR may apply. 'Personal data' includes information that is typically considered *personal* such as an employee's name, address, income details and medical condition, but also includes not always considered *personal* such as an employee's computer or device IP address device identifiers, or other 'unique identifiers.' Even if you as an employer offer certain services which give you access to such personal data, such as an IT helpdesk, server access, etc., the GDPR could apply to you.

What do I need to do?

First, you should determine whether your group of companies has EU-based employees or is otherwise processing information related to EU-based employees.

If you have EU-based employees and are processing such information, you should conduct an internal GDPR review to determine which department or which companies (e.g. IT help desk, HR, accounting, etc.) are in scope for GDPR compliance obligations, evaluate current compliance and gaps to be resolved by May 2018, and set up the necessary structure for compliance with the GDPR. The level of data protection in the EU is considered (by the EU) to be higher than in the US and US companies should be prepared for the disclosures, specific guarantees, and obligations under the

GDPR. Depending on the circumstances, the GDPR will even require US based companies with access to personal information to designate a representative based in an EU country to act as the point of contact for the relevant data protection authorities. Given the technical and detailed requirements companies may benefit from the use of targeted guidance.

Sanctions?

The global reach of the GDPR calls into question the enforceability on US-based employers. Violating the GDPR can result in penalties of up to € 20 million or 4% of the annual worldwide turnover of the company (i.e., annual worldwide gross income), whichever is higher.

Bottom line?

The GDPR will not apply until 25 May 2018, but the time for action is now. All HR departments and/or employers should carry out a data review and assess whether the GDPR is applicable and what impact it has on its activities, this in order to implement the necessary changes in time.

If you need additional guidance, an employment attorney will be able to provide guidance both on US and EU aspects of data protection law.