GDPR Is Here: Not Yet Compliant? What Employers Need to Consider

Insights
5.31.18

After much anticipation, the General Data Protection Regulation (GDPR) finally went into effect on May 25, 2018. For employers, that means some enhanced employee rights, and the risk of significant penalties for non-compliance. This includes potential maximum fines of up to 4 percent of global annual revenue or 20 million euros, whichever is greater.

Employers, even those based in the U.S., may be subject to GDPR with respect to employee data. Generally, the GDPR regulates how "Data Controllers" and "Data Processors" use and protect the personal data of the "Data Subject." The broad definitions of these terms have given the regulation extra-territorial effect:

- A "Data Controller" is an organization that collects data from EU citizens.
- A "Data Processor" is an organization, such as a cloud service, that processes data on behalf of a data controller.
- A "Data Subject" is an EU person who is the subject of the Personal Data.

This means that the GDPR applies if an employer is processing the personal data of and monitoring EU-based employees, regardless of where a company was incorporated or whether its operations are mainly outside the EU.

The GDPR's definition of protected personal data is broad. It includes "any information relating to an identified or identifiable" EU employee. This means any employee who "can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." This could include a host of information that is commonly collected and maintained by employers, including, for example, address, date of birth, phone number, photos, email address, salary information, health records, and severance data, among other things. Additionally, certain "special categories" of employee data are subject to heightened levels of protection under the GDPR. These include, for example, information regarding employees' racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and biometric and health data.

To the extent you have not already, you should immediately determine whether you are subject to GDPR, and if so, ensure you know what employee data is being collected and maintained for EU residents, why and for how long is being maintained, how and why it was collected, and what policies relate to the collection and maintenance of the security of the data, among other things. You should consider how and on what basis employee data is transferred outside the EU or to third parties, and, if employee consent to processing of personal data has been obtained, review the terms of the GDPR to determine whether the consent remains adequate.

You should also update your employee privacy policies and make sure they are available to employees, review and update employment contracts, ensure that there is a legitimate basis for processing employee data, and ensure there are processes in place for responding to employee requests, including requests to access rectify, and erase data, among other things. Under the GDPR, data controllers have 30 days to respond to subject access requests, which could be challenging for a company that does not have a good understanding of the data in its possession.

You should also be mindful of the GDPR's notification requirements in the event of a data breach. The timeframe for notification to data protection authorities of personal data breaches that are likely to present a risk to data subjects is "without undue delay," and within 72 hours if feasible, after becoming aware of the breach. High-risk breaches require notification to affected data subjects without undue delay.

What can employers who are non-compliant expect in terms of enforcement? Some data protection authorities have indicated that, to the extent companies are subject to enforcement, good faith efforts towards compliance could be a mitigating factor in determining whether and to what extent a company will be penalized. Although it is unclear how quickly or severely employers will be penalized for non-compliance, employers who are not already compliant should take immediate and demonstrable steps to ensure compliance as soon as possible.