Use Data from the EU? It's Time to Update Your Data Breach Notification Procedures

Insights
2.14.17

This post is the second in a three-part series.

With the EU General Data Protection Regulation (GDPR) looming near for organizations that process the data of European citizens, compliance is top-of-mind for multinationals doing business in Europe. The enforcement date for GDPR compliance is May 25, 2018. And according to a PwC survey of C-suite executives of certain large U.S. multinationals, more than half of the companies surveyed said GDPR is their top data-protection priority and 77% plan to spend $1 million or more on GDPR compliance.

There is no question GDPR compliance is onerous and costly, even for multinationals with large budgets and mature data governance programs. However, for those organizations that do compliance well, data privacy can be a business enabler rather than a cost center. With accountability and transparency among its foundational principles, the GDPR stipulates, among other things, that companies obtain consent of data subjects to process their personal information; provide data subjects with the right to access their personal information; ensure data subjects the right to be forgotten; and hold and process only the personal data absolutely necessary for the completion of its duties. Additionally, the GDPR requires that companies notify regulators and data subjects of most data breaches.

While the GDPR's data breach notification requirement is a key change from the EU's Data Protection Directive, which was silent on the issue of data breaches, it should not be a new requirement for many US-based companies. More than 47 U.S. states and territories have enacted legislation requiring both private and public entities to notify individuals and certain government agencies of security breaches involving personal data. Although many U.S. multinationals have adopted data breach notification protocols, these protocols will likely need to be modified to comply with the GDPR.

Under the GDPR, data controllers must notify the data protection authorities of most personal data breaches "without undue delay, and, where feasible, not later than 72 hours" after learning of the breach. Notice must be provided data subjects "without undue delay." These GDPR notification periods are much shorter than some U.S. state data breach laws which allow up to 45 days to notify subjects of a data breach in certain instances. Additionally, the scope of the information covered by

the GDPR is broader than most other U.S. state data breach laws. "Personal data" is defined in the GDPR as "any information relating to an identified or identifiable natural person ("data subject")." U.S. state data breach laws, on the other hand, generally only protect personal data that, if exposed, could lead to identify theft or financial fraud.

The GDPR, however, has a harm threshold that may provide cover for some organizations. Notification does not need to be made to the data protection authorities if the breach is "unlikely to result in a risk to the rights and freedoms" of individuals. The threshold for notification to data subjects is that the data breach is "likely to result in a high risk to [their] rights and freedoms." However, organizations that are not required to report a data breach under applicable law may still face reputational harm for their failure to do so. This point is underscored by recent backlash against UK-based Sports Direct for its failure to notify its 30,000 employees that their unencrypted personal data was improperly accessed.

Sports Direct – the UK's largest sports retailer – has come under fire recently for its handling of a data breach last year involving employee personal information. While Sports Direct reported the breach to the Information Commissioner's Office, the UK's independent body that upholds information rights, the Company allegedly did not report the breach to affected employees. It appears that Sports Direct's failure to disclose the breach may have been based, in part, on the lack of evidence that the hacker had shared the data with others.

Even if it is determined that Sports Direct did not have a legal obligation under current regulations to report the breach to employees, its lack of notice and support to its employees is a lesson on what not to do for those employers who are concerned about public and employee trust. And after May 25, 2018, these softer lessons will come with a direct financial cost as well, which, under the GDPR, will be fines of up to 2% of annual global revenues or €10 Million.

Related People

Melissa A. Dials
Partner

440.740.2108
Email