Employers With International Operations Must Take Care to Protect Employee Data

Insights
6.26.13

When is the last time your company reviewed its data protection policies? If your company employs any international employees, it may have obligations under foreign laws to have specific safeguards in place. Failure to observe a jurisdiction's data protection laws can result in staff penalties and unwelcome press coverage. Although the European Union is leading the way with a proposed comprehensive new data protection law, other countries from China to the United Kingdom, South Africa, Qatar, Dubai, and several Latin American countries are developing, or have already enacted, their own data protection laws, with many based on the European model.

The European Union
On May 31, the European Union released proposed regulations to strengthen data protection in the EU, which propose to strengthen the 1995 *Data Protection Directive*. Among other recommendations, the *Proposal for Regulation of the European Parliament and the Council on the Protection of Individuals with Regard to Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* provides for the right of individuals to be "forgotten" and not be profiled based on their personal data and also governs the transfer of information regarding EU citizens outside of the EU. The pending bill also proposed the creation of a data protection authority to assist with enforcement of the new regulations. Although the regulations have not yet been enacted, it is expected the final version will be ambitious in scope and among the most comprehensive in the world. It would be prudent for any multinational employer with European operations, customers or employees to consider the proposed regulations when drafting data protection policies.

South Africa, Qatar and Dubai are considering adopting similar measures, using the EU proposal as a template for their own regulations.

China
An American multinational company made news earlier this year when its offices in The People's Republic of China were raided and the company was criminally charged for improperly collecting personal data from individuals and selling or disclosing that data to third parties. Although there is no single, unified data protection law in the PRC, there are a number of national and provincial laws covering data protection. In 2008, the *Regulation on Employment Service and Management* was implemented nationally, and requires employers to keep personal employee data confidential, and specifically requires employers to obtain written consent before disclosing personal data.

specifically requires employers to obtain written consent before disclosing personal data.

Also on the national level, the *Guidelines for Personal Information Protection Within Information System for Public and Commercial Services* came into effect February 1, 2013. Although not law, the *Guidelines* are expected to be followed by most businesses, including multinational employers. The Guidelines set out specific requirements for employers regarding employee data collection, use, transfer, retention, and destruction. Multinational employers should note that many provinces also have implemented or are considering implementing personal data protection regulations. For example, early in 2013, Jiangsu Province enacted comprehensive data protection regulations, and penalties for violating the regulations are significant.

Steps for an Employer to Take Now

Employers without a data protection policy in place may want to consider developing a policy to protect employee and customer data. Employers with operations or employees abroad should be mindful of any data protection laws or regulations that may apply in the countries in which they operate, and should stay informed regarding the changing international data protection landscape. To that end, many multinational employers have appointed data protection compliance officers to manage policy compliance. Policies should be drafted broadly to cover not only current employees and customers, but also applicants and former employees and customers. The policies should specify the types of personal data that will be held, how it will be stored, how and under what circumstances it will be transferred, shared with third parties, and destroyed or deleted. At a minimum, the data protection policies should address security measures that will be taken to safeguard personal information. Employers may also want to consider designing a grievance procedure for employees who feel that their personal data was mishandled or misused, to enable the employer to deal promptly (and internally) with any concerns. Finally, employers should remind all employees that they should not expect privacy in their use of company IT systems, such as email, internet, mobile devices and the telephones, and that routine monitoring may occur, to the extent permitted by national or local law.

Related People

Danielle S. Urban, CIPP/E
Partner

Partner
303.218.3650
Email