wiley

NEWSLETTER

Trans-National Employers Must Harmonize Conflicting Privacy Rules

September 2002

Big and Small Alike

Global human resource privacy issues are not just for the Fortune 100 anymore. With the globalization of the United States ("U.S.") economy and the growing regulatory reach of the European Union ("EU"), even moderately-sized companies are learning that they need to understand the implications of having overseas employees. U.S. companies have been aware for some time of the requirements imposed on them by the Foreign Corrupt Practices Act and various tax and export requirements, but now the issue of privacy seems to be gaining the attention of U.S. companies operating overseas. What are the laws that affect U.S. companies, and what conduct is covered? What are the penalties for violations, and how do companies need to respond in these changing times to avoid serious pitfalls?

With more and more U.S. companies opening full-service offices, or even country- specific remote locations for sales or customer service, the need for an understanding of changing demands has become increasingly important. For now, the privacy focus seems to be on human resource issues most of all. The storage or transfer of "confidential" employee data is controlled by many of the United States' most important trading partners. Simple steps like emailing payroll data to the home office to issue checks can create a crippling violation of privacy laws. Worse still, no central legal authority dictates what conduct is required of companies operating overseas. To a large extent, each country's laws apply.

This article will outline key facets of the privacy requirements imposed by the EU and by other major U.S. trading partners. Understanding the applicable laws, however, is only the first part of addressing the issue. The second, and perhaps harder task, is formulating an employer policy that will apply to all of the organization's overseas employees, given the varied and constantly changing mosaic of applicable regulations. Isolationism is not an alternative in this competitive global economy. Therefore, companies must learn to adjust their behavior and policies to meet the changing times.

EU and Other Major Trading Countries

EU privacy laws can affect U.S. companies with overseas operations in three distinct respects. First, European subsidiaries must comply with privacy laws in the countries where they are established, and such foreign privacy laws can be significantly more constraining than their U.S. counterparts. Next, EU laws can block transfers of personal data from the EU to the United States, such as payroll information and employee

performance reviews that a European sales office wishes to send to U.S. headquarters. Finally, countries around the world are adopting the EU model of privacy protection, due in part to the extraterritorial effects of EU privacy laws. Thus, U.S. companies doing business in Canada, South America, Asia and in non-EU European countries often may face privacy obligations similar to those in force in the EU.

The EU privacy model is established through the Directive of Data Protection, which all EU Member States must implement (though three have not yet done so). The Directive creates privacy rights, gives enforcement powers to privacy regulators, and requires European companies to handle personal data under specific conditions. The Directive also generally restricts personal-data transfers to the United States, as U.S. law-which differs significantly from the European model-is not thought to provide "adequate" privacy protection. EU companies cannot legally export personal data to the United States except under one of a few sanctioned privacy regimes, such as the U.S.-EU Safe Harbor program. Further, although EU Member State laws implementing the Directive are similar, they are not uniform. Companies doing business across Europe thus face significant patchwork effects in labor and privacy laws.

EU Subsidiaries' Handling of HR Data

EU law grants European employees substantial privacy rights that any employer with operations in the EU must respect. Further, EU privacy regulators have recently made employee privacy a priority, in some cases interpreting applicable laws in ways businesses may view as unworkable. For example, employers may not be able to depend on employee consent to make data processing lawful, as regulators are inclined to see such consent as coerced. Also, regulators require employers to justify their monitoring of employees. Some regulators would limit a business monitoring of employee communications to searching for security breaches and *criminal* activity for which the employer may be vicariously liable. Indeed, recent judgments in several European countries undercut employers' abilities to monitor employee productivity (including checking for freelancing on the job), as well as to scan for disclosures of proprietary information or activity which carries merely *civil* vicarious liability (such as harassment). One group of EU privacy regulators suggested that businesses provide employees with two email accounts, one for business matters that could be monitored where justified, and another for the employee's personal use that generally could not be accessed by the employer.

Failures to comply with privacy and labor laws can carry administrative, civil and even criminal penalties, depending on how EU Member States implement the Directive. In every EU country, individuals have a private right of action to recover damages arising from violations of their privacy rights. In addition, companies may face wrongful termination suits if they fire employees based on information improperly obtained, such as the content of personal emails under certain circumstances.

HR Data Transfers from the EU to the United States

U.S. companies that receive personal data from their operations in an EU Member State must adopt a method for keeping those dataflows open. As mentioned above, transfers of personal data to the United States generally require some assurance of "adequate" privacy protection. U.S. companies have a variety of options for maintaining employee dataflows from the EU, but no method insulates U.S. companies from EU enforcement actions. Under the U.S.-EU Safe Harbor agreement, U.S. companies are generally subject only to

U.S. law and their commitment to uphold the Safe Harbor Principles, which are generally less restrictive than EU laws. But in the case of employee data, U.S. companies must agree to cooperate with EU privacy regulators and process data according to EU privacy and labor laws. Other options also give EU regulators some control over U.S. operations. For example, the EU's model privacy contract requires U.S. data importers to agree to possible audits of their U.S. facilities by EU regulators. Employers may also seek employees' consent to international data transfers, but regulators may challenge the validity of such consent if employees could perceive a disadvantage in not consenting.

Global Impacts of EU Privacy Laws

Along with U.S. companies, many businesses established outside the EU face potential data disruptions due to the Directive's restriction on international transfers of personal data. Nations around the globe are responding to this pressure by adopting the EU privacy model. Canada, Hungary, Switzerland, Australia, New Zealand, Hong Kong and Argentina, for example, now have national laws similar to the EU Directive. Some have then sought a determination from the European Commission that their national laws are "adequate," and, thus, that EU personal data may be transferred to their country freely. Consequences for U.S. businesses include the possibility of facing EU-style privacy laws across the globe, including limits on employee data processing.

Developing A Company Policy

Given these myriad regulations and the substantial penalties that they impose, how does a company formulate a policy that will apply to all the countries in which it will likely be operating? Since declining to operate overseas is not an option, companies find themselves making a choice between the lesser of two evils, formulating a single policy for all employees or having as many policies as are needed to comply with the laws of the countries in which they operate. Most companies would prefer a single policy for all employees and operations. Having varying policies and operational requirements is anathema to most companies due to the difficulty it creates for management. Having different policies for different employees, depending on where they reside, also can create resentment and tensions among the work force. Given these facts, companies often attempt to forge a single policy that will meet the requirements of all the countries in which they operate. Accomplishing this feat can be more difficult than it might first appear. By and large, the U.S. recognizes few, if any, privacy laws that apply to employees' privacy rights. By contrast, many, if not most other countries do have laws that protect employee privacy, including the information that companies usually maintain about their employees, such as salary, address, next of kin, medical information, etc.

Although a privacy solution will depend on a company's unique human resource needs and applicable law, all multinationals should consider certain steps. The first task is understanding what personal information a company collects, how this information is used, to whom it is disclosed, and whether it will be transferred internationally. Generally, companies should issue privacy policies that give employees notice about their data handling and clarify what personal use, if any, employees may make of a company's systems. Businesses should also monitor evolving hotspots among employee-privacy issues, such as video surveillance, monitoring of employee email, employees' rights to access personnel files, and limits on the background checks employers may perform on recruits. Security issues are closely tied to privacy, and while a company is examining its internal dataflows, it may also wish to assess how it is securing intra-corporate transfers of

proprietary and sensitive information.

For additional information, please contact Amy Worlton (202.719.7458).