Proskauer

International HR Best Practices Tip of the Month

December 2007

This Month's Challenge

Data protection laws in many countries can restrict the transfer of even routine HR data out of the country, even within the same company or company group.

Best Practice Tip of the Month

Learn the data protection laws in each country where the company operates, and look for "safe harbor" or other compliance mechanisms before transferring personal data out of the country.

U.S. Companies With Operations in Europe Must Comply With Data Protection Laws

The European Union's approach to data privacy is completely alien to American companies. But, as a recent decision from the French data protection agency makes clear, an American company with operations in Europe that does not learn how to play by European rules runs a serious risk of getting slapped with a hefty fine.

The U.S. has taken a piecemeal approach to privacy law, with various federal, state and local laws targeting discrete categories of data (medical and credit records, children on-line, etc.), leaving most areas of personal data processing largely unregulated. Many foreign jurisdictions (notably, but not exclusively, European Union countries) regulate personal data privacy far more comprehensively. Omnibus data protection laws regulate *all* data about identifiable people, even personal data in seemingly-innocuous databases, *e.g.,* telephone books, restaurant reservations systems, and personal weblogs. These broad data protection laws affect core aspects of business operations, including most information related to human resources, such as payroll and performance information, as well as invoicing and customer records.

Thus, the European Union's Directive governing the protection of individuals' personal data and the processing of such data mandates that the member nations adopt laws that cover *all* "processing" (defined to include even collection and storage) of data about personally-identifiable individuals. The EU Directive includes provisions addressing, among other things, limitations on the use of date, data accuracy, and data destruction requirements. The Directive is not limited to electronic or computerized data, and therefore reaches written, Internet, and even oral communications.

The EU Directive offers a blueprint for data privacy laws across Europe, but in any given situation, the Directive itself is not legally binding. As to each specific data privacy issue arising within Europe, the *relevant country's* local statute that adopts ("transposes") the Directive will determine data privacy rights and responsibilities.

The Extraterritorial Reach of the EU's Data Privacy Directive Means that *Any* Company with Operations in Europe Must Comply; Cross-Border Data Transfer Is Particularly Thorny

An important aspect of the Directive for businesses headquartered outside of Europe, such as in the U.S., is the Directive's extraterritorial reach. The Directive specifically prohibits sending personal data to any country without a "level of [data] protection" considered "adequate" by EU standards. Significantly, the EU has ruled that the United States, with its patchwork of privacy laws, does *not* possess an adequate level of data protection.

The directive authorizes a number of exceptions, legally permitting transmission of personal data outside of Europe even to a "third country" that fails to offer an "adequate level of protection."

Exceptions Permitting Cross-Border Transfers of Personal Data

The EU recognizes three “transborder data flow vehicles”: (i) a company can self-certify with the U.S. Department of Commerce that it adheres to specified data protection principles (known as the “safe harbor” system); (ii) a company can enter into “model contracts” with its European subsidiaries, agreeing to abide by mandatory data protection provisions; or (iii) a company can develop a set of “binding corporate rules” — company-drafted data protection regulations that apply throughout the company, which must be ratified by each EU member state’s data protection authority. Failure to implement at least one of these methods could result in significant liability.

Obtaining the data subject’s free, unambiguous consent to transmit his or her data overseas is theoretically another permissible way in which to transfer data to a country outside the EU — even to a country without comparable data protection law — provided that the consent specifically lists the categories of data and the purposes for the processing outside the EU. Practically speaking, however, obtaining consent to legitimize a transfer overseas is often not an available alternative for employers; in the employment context, because of the imbalance in bargaining power between employer and employee, consents may be presumed *not* to have been freely given.

Also, of course, there is no prohibition against transmitting genuinely *anonymized* data out of the EU. Where the identity of the data subject is impossible to determine, the data transmission falls outside the scope of the directive.

European Countries Turn Their Eye To U.S. Companies Operating In Europe

EU data protection authorities are increasingly scrutinizing European subsidiaries of U.S. companies. As a result, a French subsidiary of a U.S.-based company recently became the first local branch of a U.S. company to be fined for data protection violations in France. France’s data protection agency, *La Commission Nationale de L'Informatique et des Libertes* (CNIL) levied a fine of 30,000 euro (about $42,462) against Tyco Healthcare after it both ignored CNIL’s requests for clarification about one of its human resource databases and then made misrepresentations concerning the database to the regulatory agency. When Tyco Healthcare sought to register the database, pursuant to the requirements of French data protection laws, it represented to CNIL that its purpose was to assist with the processing of employee salary information. CNIL requested further information about transborder data flow, the nature of the data base, its functions, and security features. The company failed to respond to the agency’s repeated requests for clarification, and then finally represented to CNIL that the database had been suspended. After an investigation, the data protection agency learned that not only was the relevant database still active but its use was much more widespread than the company had earlier represented.

The Tyco Healthcare case should provide a strong wake-up call to U.S. multinationals with operations in Europe (and particularly France) underscoring the importance of compliance with European data protection laws, which may be unfamiliar to U.S. based companies. Moreover, any multinational with a global HRIS (Human Resources Information System) that transfers data from Europe to another country (other than Switzerland, Argentina, and Canada, which have been accepted by the EU as possessing laws that provide an adequate level of data protection) should ensure that it sends data overseas pursuant to an
EU-sanctioned method and, when in doubt, should consult with an attorney to ensure full compliance with EU legal requirements.

Cécile Martin
33.1.53.05.69.26 – cmartin@proskauer.com

Cécile Martin, primary author of this newsletter, is an associate in the Labor and Employment Law Department in the firm's Paris office. She has experience in all employment law aspects of corporate restructurings, redundancy procedures, negotiations with employee representative bodies (personnel delegates, works councils, health and safety committees, unions) and French Labor Authorities (Labor Inspector, Ministry of Employment). Prior to joining Proskauer, she served as in-house counsel for the legal department of the French Data Protection Agency (C.N.I.L.). She has participated as a speaker for the Technology in Practice and in the Workplace Committee of the American Bar Association on several occasions.

Related Professionals

- **Howard Z. Robbins**
  Partner