# Developing Global Data Privacy Policies for HR Data

Mar 01 2008

Posted By: Mark F. Foley

Practice Area: Labor and Employment & Information Technology, Data Privacy and Security

Multinational companies are enthusiastically deploying globally integrated Human Resources Information Systems ("HRIS"). CIOs and other managers need to understand and address the data privacy compliance issues these systems create. Failing to do so could result in significant sanctions, expensive system redesigns, or orders limiting or prohibiting use in certain countries. This is the first in a two part series identifying how these privacy issues arise and the three ways companies can design their systems to satisfy myriad and often conflicting global data privacy requirements.

PeopleSoft, SAP, Oracle and other large integrated databases all offer benefits to multinational corporations. They can enable senior management to get instant views of personnel compensation and performance anywhere in the world. Companies can better insure that individuals performing comparable work receive equivalent compensation wherever they reside. Success in meeting goals for hiring, compensation, and promotion of women and minorities can be assessed across the organization, rather than in geographic submarkets. One such technology platform may replace several older systems providing lower performance while requiring higher aggregate licensing, maintenance, and support costs.

These benefits arise out of the integration, expanded access, and broader use of personally identifiable information once limited to local activities, raising concerns among data protection authorities.

Today, these concerns are most frequently raised by data protection authorities in the European Union ("EU"). The EU leads the world in adopting broad, stringent data protection laws. This results from the European Commission's adoption of Data Privacy Directive 95/46 EC, which required all EU Member States (France, Germany, UK, etc.) to adopt national legislation providing at least a minimum level of protection for privacy interests in personal data. These laws apply to all "personally identifiable information" - i.e., information which alone, or in combination with other lawfully available information, could be used to identify a specific individual ("PII"). Thus names, governmental identification numbers, employee IDs, IP addresses, email addresses, DNA samples, and collections of descriptive information all identify individuals or make them identifiable.

The European laws are based on the premise that the subject of such data has the right to control its collection, use, dissemination, transfer, destruction, and other "processing," unless the law specifically authorizes or commands use without the data subject's consent. The laws require all those determining what information is going to be collected and how it is going to be used – the data controllers – to adhere to broad data protection principles when they process PII and to provide the data subjects specific procedural rights. The data controller, such as an employer, must take approved steps to assure that data privacy and security mechanisms continue to provide an adequate level of protection when the data are transferred outside of Europe. Without such protections in place, transfers outside of Europe are prohibited.

In a typical HRIS implementation, data collected in Europe and other countries will be stored and processed on servers located in the U.S. Even if no one accesses the data there, the transmission, storage, and processing on those servers constitutes a transborder transfer of the data. When an executive at the U.S. headquarters accesses data held on servers located in France, there is a transborder transfer. When an HR representative managing global performance evaluations looks at that data while traveling in Hong Kong, yet another transborder transfer occurs. If EU data transferred to the US headquarters is then handed to a vendor who provides contractual data processing services, yet another transfer has occurred. As you can now see, an integrated HRIS system inherently involves transborder data flows with multi-jurisdiction ramifications.

Privacy rules in the U.S. are quite different from those in Europe. Data subjects in the U.S. are not always presumed to own the data about themselves and do not have broad, generalized data privacy rights like those provided in the EU. They tend to be designed to protect specific kinds of data (e.g., health data covered by HIPAA or financial data covered by the Gramm-Leach-Bliley Financial Services Act ("GLB")) or to control specific types of uses (e.g., CANSPAM prohibition of sending spam to email addresses and the Federal Trade Commission's "Do Not Call" rules prohibiting certain telephone marketing calls.

Although these sector based laws appear to be quite different, they are in fact based upon the same fundamental privacy principles that are at the root of the EU Directive and other privacy laws worldwide. For example, EU law requires that data subjects receive notice of the data controller's activities – what data are collected, how are they used, with whom are they shared? Similarly, HIPAA and GLB require a covered health care provider or a financial services company, respectively, to provide consumers with notice of what information is collected, how it is used, and with whom it may be shared.

In addition to the broad general data protection statutes adopted to implement the EU Data Privacy Directive, many European countries have other sources of privacy law. For example, France recognizes a "fundamental human right" of privacy in one's correspondence, including email. Consider how that conflicts with the typical U.S. based company's email policy that says users should have no expectations of privacy with regard to anything created, sent, received, or viewed using company computer systems!

In even greater contrast to the EU system, some countries where many Wisconsin based multinationals operate, such as Taiwan, Singapore, Malaysia, China, and Mexico, have little or no data protection law and no limits on transborder data transfers.

In Part Two of this two-part series, I'll discuss the three ways that multinationals operating across multiple international jurisdictions can design a largely uniform data privacy policy for all its employees.

---