

CLIENT ALERT

August 2, 2007

Europe Clamps Down on Data Protection Violations: U.S. Multinational Fined for Cross-Border Data Transfer

For the first time, a U.S. multinational organization has been fined for violations of the E.U.'s Data Protection Directive, following a recent clampdown by European data protection authorities on breaches of the E.U.'s strict data protection regime. France's data protection authority, *La Commission Nationale de l'Informatique et des Libertés* (CNIL), recently fined the local French subsidiary of U.S.-based Tyco Healthcare for €30,000 (more than \$40,000) after discovering that Tyco's human resources database was using personally identifiable information, more extensively than the company had declared, and improperly transferring this personal data overseas to its U.S. headquarters.

Europe Clamping Down

CNIL's zealous enforcement should be seen as just the tip of the iceberg. Collision with the European authorities can result in significant fines, sanctions, negative public exposure, as well as civil and criminal liability. Greater perils loom ahead as the European Data Protection Supervisor has called for stronger and more expansive enforcement programs within the E.U.'s Member States. The United Kingdom's own Information Commissioner is also pushing for additional sanctions and auditing power, and has been actively pursuing all forms of data protection infringement. These are hazardous waters to navigate for U.S. multinational organizations, particularly because the European data protection laws apply to all cross-border transfers of personal data, even transfers within a single multinational entity. As the data-flow between U.S. companies and their foreign subsidiaries increases, so too does the risk of violating the E.U. regime, which may be unfamiliar to U.S.-based companies.

Notably, the Directive prohibits the transfer of personal data (whether employees' or clients') from an E.U. Member State to any entity based in a country outside of the European Economic Area (EEA), whose laws do not provide an adequate level of protection for the transferred data. The E.U. has rejected the United States' lax data protection laws for failing to ensure an "adequate level of protection", and, consequently, U.S. corporations are prohibited from transferring personal data from the E.U. to the U.S. unless certain E.U.-approved safeguards have been put in place to protect this data.

Risks of Global Human Resources Databases

The Tyco case exemplifies the risks for U.S.-based multinationals of using sophisticated global databases that permit the seamless international transfer of personal data. Tyco's clash with the French authorities began when it registered (as required by French law) its global Human Resource Information System (HRIS), but only provided a nebulous description of the purposes for which the data was stored. CNIL requested more details about this management tool, the nature of the cross-border transfers, and the security measures that Tyco had implemented to safeguard the data; but it received scant replies and was eventually told that Tyco had stopped using the database. Dissatisfied with Tyco's response, CNIL launched an on-site, surprise

inspection of Tyco's French offices. Through this investigation, CNIL discovered that not only was Tyco's database active, but contrary to its representations, and like many global HRISs, the database also contained extensive personal information about its employees, including stock-options, compensation levels, and professional skills and preferences. These purposes went significantly beyond the descriptions of use that Tyco had registered for its HRIS.

CNIL drew attention to the fact that Tyco was using its HRIS to transfer personal data to the U.S. and had never received CNIL's approval for the international transfer of this information. By fining Tyco, the E.U. authorities have sent a warning shot to any multinational with a global HRIS that engages in cross-border data transfers, to ensure that it transfers such data in accordance with E.U. sanctioned methods described below.

The Options for U.S. Multinationals Engaging in Cross-Border Data Transfers

The Tyco case should serve as a wake-up call to U.S. multinationals and highlights the importance of complying with European data protections laws, which, to date, many U.S. corporations have kept on the back burner. Of particular importance to U.S. multinationals will be the ability to preserve their cross-border transfer data transfers, and, to this end, the E.U. has approved the following methods to effect such transfers:

- **Self-Certification under the Safe Harbor Program.** Under the Safe Harbor program, companies have been able to voluntarily adhere to a set of seven principles: Notice, Choice, Transfers to Third Parties, Access, Security, Data Integrity, and Enforcement. These principles are recognised by the E.U. as providing adequate protection and, therefore, meeting the requirements of the E.U. regarding transfers of data to the U.S. Participating companies must renew their self-certification annually, and certain industries—such as telecommunication carriers, banks, and insurance companies—may not be eligible for this program. Safe Harbor's two greatest drawbacks for U.S. multinationals are (1) that the company is bound by actionable representations to both the FTC and E.U. authorities in relation to its adherence to the Safe Harbor Principles, and (2) it is therefore subject to enforcement and sanctions from both authorities. Additionally, the solution is not global, because it only applies to data transfers from the E.U. to the U.S.
- **Incorporating the Standard Contractual Clauses.** Companies involved in the transfer of personal data can enter into model contracts between the legally independent entities involved in the transfer. Contractual clauses should establish adequate safeguards by creating obligations similar to those in the Safe Harbor program. However, such clauses may result in greater liability for the data controller and additional due diligence obligations. Unfortunately, their very nature precludes them from being used for intra-group transfers within a multinational corporation.
- **Adopting Binding Corporate Rules.** A multinational can develop a set of binding corporate rules that govern data protection and apply to all intra-group transfers of personal data outside of the EEA. The rules must be approved separately in each Member State where the multinational has an office, and the applicant must describe the data protection audit plan, the processing and flows of information, the data protection safeguards, and mechanisms for reporting and recording changes, as well as demonstrate that these rules are binding both internally and externally. Such rules could theoretically solve all data transfer issues within a global company, but they can involve certain practical difficulties depending on the size of the multinational. Incorporating approved rules may cost millions of dollars and years of development

time. To date, only two companies, General Electric and, more recently, Phillips, have had such rules approved. A movement to reform the Binding Corporate Rules guidelines is underway.

The Bottom Line

European data protection authorities are clamping down, and the Tyco case serves as a timely reminder to U.S. companies of the requirements and reach of E.U. data protection law. Aside from fines and negative publicity, companies violating E.U. law can face civil and criminal liability. However, all transfers of personal data from the E.U. can be preserved, but U.S.-based companies should actively adopt one of the E.U. approved options and, in so doing, give a confident message to employees, customers, and competitors. ■

For further information on the practical steps that can be taken to achieve compliance with the E.U. data privacy regime, please contact:

Ieuan Jolly

+1.212.603.6553.

ijolly@thelen.com

©2007 by Thelen Reid Brown Raysman & Steiner LLP. This article has been published as an information service for clients and friends. Please recognize that the information is general in nature and must not be relied upon as legal advice. The authors, or your Thelen attorney contact(s), would be happy to discuss the information in this article in greater detail and its application to your specific situation. We welcome your comments and suggestions.