ASAP™
A Littler Mendelson **Time Sensitive** Newsletter

in this issue:

MAY 2007

The French Data Protection Authority assesses the first-ever fine on a U.S.-based employer for improper cross-border transfers of human resources data. The fine highlights the need for U.S.-based multinationals to comply with the European Union's strict data protection requirements.

International Employment and Labor Law

A Littler Mendelson Newsletter specifically for International Employment and Labor Law

French Data Protection Authority Fires Warning Shot to U.S. Multinationals: U.S.-Based Employer Fined for Improper Transfers of Employee Data to the U.S.

By Philip L. Gordon and Timothy A. Rybacki

In what may foreshadow a new era of more aggressive enforcement, France's data protection authority - *La Commission Nationale de L'informatique et des Libertés* (CNIL) - recently fined Tyco Healthcare France (THF), the local subsidiary of a U.S. multinational organization, €30,000 (approximately $41,000) for, among other things, improperly transferring employee information to Tyco's U.S. headquarters. The fine appears to be the first imposed on a U.S.-based company accused of unlawful cross-border transfers of human resources data. The French government's enforcement action coincides with recent public declarations by other European data protection authorities, calling for more aggressive enforcement of the European Union's strict data protection regime.

The Tyco Decision Exemplifies the Potential Risks of Global Information Sharing

The enforcement action against Tyco circled around a human resources tool that has become increasingly common, if not ever present, among multinational businesses - a global human resources database. When Tyco initially registered the database as required by French law, the company stated broadly, but somewhat vaguely, that it was engaging in "data collection and processing for the purpose of 'managing the careers of [Tyco's] international employees.'" Finding this description insufficiently detailed, CNIL asked Tyco to provide "a description of the exact purposes for which the information was sought, the precise cases in which personal data is sent to Great Britain and the United States, exact places of installation of servers and systems, precise purpose of the data storage, exact recipients of the data, safety measures ensuring the data's confidentiality, and the shelf life of the data."

Tyco declined to respond to several requests by CNIL for this more detailed information about the database. Then, Tyco informed CNIL that the company had suspended use of the database pending a corporate reorganization. Apparently frustrated by Tyco's failure to provide the requested information, CNIL exercised its authority to conduct an on-site investigation at Tyco Healthcare France.

CNIL's investigation uncovered that the employee database not only was very much still in use but, contrary to the description in Tyco's initial registration, was "an essential management tool, at the world level." CNIL found that, like many global human resources databases, Tyco's database is used to manage a broad range of information, including stock-options, vocational training, compensation levels, and employees' willingness to perform work for Tyco in countries other than France.

Notably, CNIL confirmed that Tyco was using the database to transfer human resources data to the United States, although Tyco had never received CNIL's approval for the cross-border transfer of this information. In addition, Tyco did not explain the purposes of these transfers to CNIL. Before issuing the €30,000 fine, CNIL chided Tyco for its "obvious failure to take seriously" CNIL's concerns regarding the employee database.

The penalty imposed on Tyco highlights the often overlooked risk that U.S.-based, multinational employers face when they

deploy sophisticated database technology that permits the seamless exchange of personnel information across national borders. The national laws implementing the E.U.'s Data Protection Directive generally prohibit the transfer of employees' (or customers') personal data from an E.U. Member State to any entity outside the E.U. - *even an entity within the same corporate group* - which is located in a country whose laws do not provide an "adequate level of protection" for the transferred data. According to the E.U., the U.S. does not provide an "adequate level of protection." Consequently, U.S. corporations cannot lawfully transfer employee information from the E.U. to the U.S. without first taking steps (described below) to provide an adequate level of protection for the information.

The Tyco decision also reflects a growing sentiment among E.U. authorities that the Continent's data protection laws, including those governing cross-border data transfers, have been inadequately enforced for too long. By way of illustration, the European Data Protection Supervisor, who is responsible for overseeing implementation and enforcement of the Directive, recently listed as a particularly high priority strengthening the enforcement initiatives of E.U. Member States. In consonance with this position, the United Kingdom's Information Commissioner recently pressured the U.K. Home Affairs Committee for greater enforcement authority and strengthened auditing powers, particularly with respect to organizations responsible for the safe handling of employees' and customers' personal data. In sum, if this trend toward increased enforcement activity continues, the Tyco decision may well be the first of many such enforcement actions against U.S. multinational companies.

Implications of the Tyco Decision for Employers

CNIL's decision to fine Tyco should serve as a strong signal that the current enforcement environment in Europe has shifted to the point that U.S.-based employers can no longer afford to keep the issue of compliance with E.U. data protection laws on the back-burner. Employers should immediately address compliance with the E.U.'s data protection laws. Particularly, employers should recognize that procedures for collecting and transferring employee data that are necessary to efficient human resources management in the United States may expose the organization to civil and criminal liability in Europe.

U.S.-based companies, though, are not without several options to preserve their cross-border data flows. The available options include the following:

Certifying to the U.S. Safe-Harbor Accord: The Safe Harbor Accord consists of seven data protection principles that the European Commission has determined provide an "adequate level of protection" for personal data. By certifying adherence to the principles outlined in the Safe Harbor, a U.S. business can meet the E.U. Data Protection Directive's "adequacy" requirement, even though the U.S., on a national level, does not. Once a U.S. organization certifies that it is in compliance with the Safe Harbor Principles, the data protection authority of each E.U. Member State must automatically approve transfers of personal data to that organization. It is important to note that certification to the Safe Harbor constitutes an actionable, public representation to the U.S. government that the organization will adhere to the promised privacy protections and, therefore, is subject to administrative enforcement by the U.S. Federal Trade Commission. The organization also must agree to cooperate with E.U. Member States' data protection authorities and to abide by their enforcement orders. As of the end of 2006, approximately 1100 companies had certified to the Safe Harbor.

Binding Corporate Rules: Under this option for preserving cross-border data flows, a multinational business organization adopts a uniform set of data protection rules applicable to all intra-group transfers of personal data originating from the E.U.. Once approved by the local E.U. Member State, these binding privacy rules will be deemed to provide an adequate level or protection for data transferred from that particular E.U. country to any member of the corporate group in any non-E.U. country. This option is particularly suited for transfers of human resources data because it applies exclusively to intra-group transfers, and, unlike the U.S.-E.U. Safe Harbor Accord, may also provide a truly "global solution" for large multinational companies with operations in a substantial number of countries. The corporate group must take steps to ensure that these rules are binding internally on a practical level. Notably, binding corporate rules must also be structured in a way that would permit *judicial* enforcement in each E.U. country where they are effective-not just administrative enforcement by national data protection authorities. The largest drawback to this option may be the difficulty in gaining approval from individual Member States. At present, a company's binding corporate rules must be individually approved by each national data protection authority, and the requirements for approval commonly vary quite significantly from Member State to Member State. European data protection authorities, however, are working to develop mechanisms that will streamline the approval process.

Model Data Transfer Contracts: As a third option, multinational employers may be able to preserve their cross-border data flows through contractual agreements between the entities sending and receiving the human resources data. In these contracts, the entity receiving the information agrees to abide by data protection provisions similar to the Safe Harbor Principles when it processes the transferred data. For many organizations, however, this option may not be available with respect to human resources data because the European organization transmitting the information and the organization receiving the information must be legally independent entities in order to execute a binding, non-illusory contract.

Conclusion

As the Tyco decision demonstrates, the potential cost of failing to comply with E.U. data protection laws can be substantial. Nevertheless, compliance with the E.U.'s relatively onerous data privacy regime need not require that a business abandon or redirect its cross-border data flows. U.S.-based employers should actively consider implementing solutions, such as certification to the Safe Harbor Accord or the development of binding corporate rules, which would simultaneously preserve information flows and establish compliance with E.U. data privacy laws.

Philip L. Gordon is a Shareholder in Littler Mendeson's Denver office and Timothy A. Rybacki is an Associate in Littler Mendelson's Houston office. If you would like further information, please contact your Littler attorney at 1.888. Littler, info@littler.com, Mr. Gordon at pgordon@littler.com, or Mr. Rybacki at trybacki@littler.com.