FOR METRO AREA IN-HOUSE COUNSEL

GC New York

New York Law Journal

ALM

Thursday, June 21, 2007

Privacy and Data Protection

Collecting Employee Data in Europe

BY WILLIAM A. TANENBAUM
AND CATHERINE YOUSSEF KASSENOFF

MANY U.S. businesses are aware of the strict requirements in European privacy law that apply to the collection of information from their European consumers. The same restrictions apply to the collection of data from companies' own European employees. The use of new technologies such as company intranet sites and encrypted e-mail systems provide business advantages but complicate the application of European privacy law requirements to employee data.

The starting point for analyzing employee data is the broad scope of protection given to "personal data" under the Directive issued in 1995 by the European Commission on "The Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data" (Directive 95/46/EC). The directive has been implemented through the national laws of the member countries in the European Union, which was recently expanded to 27 countries, and also in Iceland, Norway and Liechtenstein, which are not members of the EU. These 30 countries are known as the European Economic Area. For convenience, in this article these countries will be referred to as the "European countries" and the privacy laws of these countries will be referred to as "European law."

Companies must grapple with multiple layers of consent.

Personal data is information about a living individual or about an individual who can be identified from that information alone or in conjunction with other information. Personal data can be processed—which in this context includes collected—only if the "data subject" (the living person who is the subject of personal data) has been told what data will be collected and how it will be used, there is a legitimate purpose for collecting the data, the data subject has given his or her unambiguous consent to the collection and use of the information collected, and certain other requirements have been met.

An important subset of personal data in the employment context is "sensitive data." While the exact definition can differ by country, sensitive data includes racial or ethnic origin; religious beliefs or beliefs of a similar nature; membership in a trade union; a physical or mental health condition; sexual orientation; the commission or alleged commission of a crime; and proceedings for any criminal offense committed or alleged to be committed by the data subject and the outcome of such proceedings. Processing sensitive data requires a higher level of consent, namely, explicit consent. By its nature, sensitive data is likely to be involved in employment matters.

A complicating factor is that in European countries the employer/employee relationship is considered to be inherently coercive, and consent given in a coercive context with respect to sensitive data is not always deemed freely given. Indeed, in some European countries, such as Italy, employers cannot collect sensitive data from employees without first obtaining permission from the country's Data Protection Authority, or DPA.

As a result, the emerging business practice of using a company intranet site to allow internal job candidates to post their resumes creates a dilemma for employers operating in countries that require them to obtain DPA approval before they process sensitive employee data. In this scenario, the employee's submission of the resume may be deemed to constitute processing by the employer of employee sensitive data.

The dilemma is that in theory the employer is supposed to have obtained DPA approval to process a resume before the employee posted it, but the employer may not have known of the need to seek approval until after the employee unilaterally submitted his or her resume to the site. It is not yet clear what steps by employers will be deemed an effective legal solution in this fact pattern in countries where DPA approval is required and where explicit employee consent without DPA approval is considered insufficient.

An emerging practice adopted by some employers is to include a notice on the site that requires applicants to redact sensitive data before submitting their resumes. If the employee fails to do so, the employer can reject and return the resume and direct the employee to remove the data before the resume will be considered.

William A. Tanenbaum *is chair of the technology, intellectual property & outsourcing group at Kaye Scholer and head of the firm's privacy practice.* **Catherine Youssef Kassenoff**, *former assistant U.S. attorney in the Eastern District of New York, is senior privacy counsel at a financial institution.*

The foregoing example, while extreme, illustrates the breadth of activity that will be deemed to constitute data collection for European employee data collection purposes. Another common employer practice is the use of intranet sites to track hours worked by employees. The purpose of tracking the hours is to allocate them to internal or client projects. The intranet sign-on function will generally require the employee to submit his or her name and e-mail address for identification and verification purposes. This data, however, constitutes personal data (although it probably does not constitute sensitive data).

Even though the site is operated by the employer so that it can track and allocate employee hours, is it deemed to be collecting the personal data of those employees whose hours are being allocated? The short answer is yes; there is no de minimis exception for the collection of personal data under European law. Thus, the employer must affirmatively obtain consent from the employee to collect the personal identification and verification data using means that comply with applicable processing requirements.

A similar situation arises when employers use encrypted e-mail systems to protect the confidentiality of employee communications. Even though the core encryption part of the technology does not collect data, the part of the system that holds and organizes the e-mail messages, which happen to be encrypted, is deemed to be collecting the employee personal data that appears in the e-mail messages. As a result, the employer must obtain consent from employees to collect this data.

Obtaining Consent

How is consent obtained from employees? Without addressing sensitive data for now, we recall that European law considers the employer/employee relationship to be inherently coercive; the result under European law with respect to personal data is that the employee's consent must be "unambiguous." Under European law, an employee cannot provide consent to the use of personal data for different purposes in a single, multi-purpose consent form. Instead, unambiguous consent is deemed to require specific consent to each of the purposes for which the information will be collected and used.

The mechanism for obtaining consent for multiple purposes has been addressed by an advisory body established under Article 29 of the directive and known as the "Article 29 Working Party." The Working Party was established to provide advice regarding the harmonization of data protection rules and is composed of national Data Protection Commissioners from EU countries and a representative of the EU Commission. The Article 29 Working Party issued a paper in November, 2004 in which it advised that notices provided to employees should be "multi-layered." The Working Party contemplates a document with multiple parts whereby key terms are not to be buried in a single, long notice provision. Rather, there are to be individual "layers" for each of the purposes (or business functions) for which personal data is being collected, and the notice in each layer "must communicate the information necessary for the individual to make an informed decision at that point in time."

Affirmative consent is another means of achieving unambiguous consent. In the online context, a click-through agreement can provide the basis for affirmative consent. The click-through agreement requires the employee to read the consent terms and then accept or decline to accept the terms under which personal data will be collected, used and transferred. The online system of collecting information cannot be used unless affirmative acceptance of the terms is provided by the employee.

Note that affirmative consent differs from notice in that notice alone is deemed to be informational only and does not require any manifestation of agreement from the reader. In addition, having the computer system record the manifestation of the employee's agreement provides electronic evidence of consent, and thus strengthens the employer's argument that it obtained the employee's affirmative consent before any of his or her personal data was collected. It also establishes that consent to a specific use of the data was provided.

In addition, to secure proper consent, an employee must be given notice in a language he or she understands. The requirement for translation should be given careful attention by companies doing business on both sides of the Atlantic. For example, the French language in Quebec is considered sufficiently different from French in France that notices in one "language" must be translated to the other in order for the consent to be deemed valid.

There is also a Works Council aspect to employee consent. Works Councils are "shop floor" organizations that constitute the local or company-level complement to a national trade union in Europe. Works Councils often have contractual arrangements with companies that require the companies to obtain Works Council approval to the procedures to be used by an employer to obtain the consent of the employees with respect to data collection.

Finally, there is an outsourcing component to employee data collection in Europe. In outsourcing, it is common for the company receiving outsourcing services to conduct or ask the vendor of outsourcing services to conduct background checks on the vendor employees who will have access to the personal data of the company's customers in the course of providing outsourcing services. This is to screen out vendor employees with criminal records. However, information concerning the commission or even the allegation of a criminal offense constitutes sensitive data under European law.

The restriction on collecting sensitive data relating to criminal offenses makes it very difficult to conduct the type of criminal background checks that are typically conducted outside of Europe. The issue has gained greater importance now that Eastern European countries have become virtual "offshore" outsourcing countries for Western European companies and become members of the European Union (and its citizens subject to employee data privacy protections). The result is that the due diligence represented by criminal background checks is not available for European-based employees.

> European law considers the employer/employee relationship to be inherently coercive; the result under European law with respect to personal data is that the employee's consent must be 'unambiguous.'

Conclusion

The application of European privacy laws to the collection of consumer data is well known to most U.S. companies doing business in the EU. These laws also apply to the collection of data from a company's existing or prospective employees, and require companies to comply with privacy restrictions with regard to their internal as well as customer operations.