Maintaining Employee Privacy Across Jurisdictions

This article first appeared in *Employment Law360*, November 22, 2011

by Scott E. Landau and Bradley A. Benedict

Scott E. Landau
Executive Compensation & Benefits
+1.212.858.1598
scott.landau@pillsburylaw.com

Bradley A. Benedict
Executive Compensation & Benefits
+1.212.858.1523
bradley.benedict@pillsburylaw.com

Scott Landau is a partner in Pillsbury's New York office. He represents private equity clients and public companies in acquisitions, divestitures and restructurings within the U.S. and internationally and counsels clients on designing executive compensation and nonqualified plan arrangements. Bradley Benedict is an associate in Pillsbury's New York office, where he helps advise on a variety of pension, profit-sharing, welfare and other employee benefits matters.

Employers collect a substantial amount of personal information about their employees. Companies need to be aware of their obligations under the profusion of data protection laws and regulations that govern the collection, use and transfer of personal information.

This is an especially daunting task for companies that have operations subject to the laws of multiple jurisdictions, as requirements vary widely from country to country and even from state to state. Here, we summarize some basic concepts executives, inside counsel and human resource managers should consider under current data privacy laws.

Companies use employees' personal information for a variety of purposes, from evaluating applicants during the hiring process to administering payroll and employee benefit plans to managing separation and other post-employment benefits.

As more employers adopt enterprise-level information management systems and outsource certain human resources administration functions, increasing amounts of personal data is being transferred and shared within and between organizations.

Maintaining compliance with applicable data privacy laws is a responsibility employers cannot afford to overlook.

Protected Information

As a rule, only personally identifiable information (personal data) is afforded special protection by data privacy laws. This usually includes one or more types of data that identifies or is linked to an identifiable living individual, e.g., name or Social Security number. In some cases, it includes a combination of such information that could potentially identify an individual, e.g., birth date, gender and postal code taken together.

Many, but not all, data privacy laws exempt personal data that has been encrypted. Certain types of "sensitive data" are often given enhanced protection under comprehensive data protection regimes.

Sensitive data may include, for example, race, ethnicity or national origin, political opinions or associations, union membership, sexual orientation, marital status, health-related information and criminal history.

It should be noted that data privacy laws are not restricted to protecting active employee information, so companies' obligations extend

to any nonemployee groups whose personal data they may acquire, such as clients and customers, but also job applicants, consultants, independent contractors and terminated or retired employees.

Data Privacy Laws Around the World

United States

A few U.S. federal statutes protect specific types of personal data. The most important of these for employers are the Health Insurance Portability and Accountability Act[1], covering certain health-related information; the Genetic Information Nondiscrimination Act, which applies specifically to genetic information; and the Fair and Accurate Credit Transactions Act, designed to protect consumer credit information.

In addition, most U.S. states have laws concerning data security and security breach notification.[2]

Many of these laws are identity-theft protection measures that generally impose an obligation to protect Social Security numbers and similar personal data against unauthorized use or disclosure and require secure destruction of such data.

One state has gone a step further: since March 1, 2010, Massachusetts requires most companies to adopt a written security policy that meets certain standards to protect a broad range of personal data collected from customers and employees who reside in the state. A compliant plan requires not only security measures, such as encryption of personal data stored on portable devices, but also training and oversight of vendors who have access to the data.

Although U.S. law is trending toward stricter protection of personal data, the laws in other countries are often much more extensive than even the strictest U.S. standards.

Many U.S. companies that do business globally will need to go beyond the requirements of U.S. law to facilitate the lawful flow of personal data into the U.S. from countries with more restrictive rules, as further discussed below.

European Economic Area

The European Union's data protection directive 95/46/EC recognizes personal data privacy as a fundamental right and establishes a comprehensive scheme to protect such information, as implemented by the enacting legislation of the nations comprising the European Economic Area.

These extensive rules cover the collection, processing (including storage) and transfer of personal data in any form.

Among other things, requirements include the adoption of reasonable security measures, an obligation to notify and, in some cases, obtain consent from individuals about the collection, protection, use and disclosure of their personal data, and may include notice filings with local data-protection authorities.

Because the EU directive merely sets forth minimum standards, there is considerable variability in the specific restrictions imposed and degree of flexibility allowed under the laws of individual EEA countries.

The EU directive also generally prohibits transferring personal data, without consent of the individual, to countries whose laws do not ensure an "adequate" level of protection, unless the receiving entity agrees to model contractual provisions providing for such protection.

U.S. laws are not deemed sufficient in this regard, but the EU and U.S. Department of Commerce created a self-certification safe harbor program whereby U.S. companies can pledge to adhere to seven principles to become eligible to receive personal data from EEA nations.[3]

These safe harbor principles relate to:

1. Notification requirements as to personal data collected, how it will be used and who will have access;
2. Opt-out opportunities for the use of personal data and opt-in requirements, i.e., obtaining prior consent, to use sensitive data;
3. Restrictions on transfers to third parties, e.g., benefit plan administrators, to ensure the third party maintains security measures consistent with the safe harbor principles;
4. Taking reasonable security precautions against loss, misuse and unauthorized access;
5. Limiting use to necessary or consented-to purposes;
6. Allowing individuals to access and correct their personal data; and
7. Implementing an enforcement mechanism meeting certain standards, e.g., submitting to the dispute resolution body of the applicable EEA nation.

Non-EEA Countries

Legislation concerning data protection varies greatly in other countries. Some have comprehensive data protection laws in the manner of the EU directive, including Argentina, Australia, Canada, China and Japan.

Mexico and India also recently enacted broad data privacy legislation. Some countries have laws of limited applicability, focusing on specific types of information or processes, while others have little or no legislation in this area.

Other Considerations

Employers should consider all legal requirements, whether local, state or provincial or nationwide, that may impact their data privacy policies and procedures. These may include, for example, employee record-retention rules, "whistleblower" statutes and restrictions on monitoring or surveillance of employee activities and communications.

Certain processing or handling of personal data, and changes to a company's privacy policies, may require disclosure to and/or consultation with unions or works councils representing affected employees, particularly in the EEA.

Penalties and Compliance

Many data privacy laws explicitly provide affected parties with personal rights of action for statutory violations. Civil fines are also common, and some laws permit criminal prosecution for egregious cases.

For example, fines for a HIPAA privacy violation range from $100 to over $50,000 per violation, up to an annual cap as high as $1.5 million, depending on the level of culpability, but offenses committed knowingly can result in criminal prosecution.[4]

Further, employers whose employees' identities are stolen due to knowing violations of FACTA may be held responsible for minimum statutory damages of up to $1,000 per employee, plus punitive damages and attorney's fees, and can be subject to civil fines of up to $2,500 per employee in enforcement actions brought by the Federal Trade Commission and additional amounts from state authorities.

The EU directive grants data subjects a private right of action for data privacy law violations, and local data protection authorities have enforcement powers that include the imposition of fines, which can be severe.

Agencies in France, Spain and Germany have levied fines of €1 million or more. In Spain, where enforcement has been particularly aggressive, a recent law change lowered the minimum and maximum penalties for various violations and provides for nonmonetary resolution of minor infractions.

Criminal penalties also exist in some EEA countries for certain offenses. Outside of the statutory penalties and claims, companies need to be concerned about civil suits for damages and the adverse effects of personal data security breaches on public and employee relations.

Minimizing Risk

Data protection laws tend to be complex and, in part because they are relatively new, there is not a great deal of interpretive guidance on compliance matters.

Companies seeking to minimize their exposure from legal violations and security breaches involving employee personal data should:

- Consider adopting data privacy and protection best practices that aim to limit the amount of personal data they collect, process, transfer and store;
- Secure personal data collected, in all formats in which it is kept;
- Limit access to personal data to the extent practicable and provide training to staff who handle personal data;
- Ensure third parties receiving personal data are subject to and apply appropriate security measures;
- Prepare for security breaches involving personal data;
- Maintain accuracy of the personal data collected and processed; and
- Monitor compliance with all applicable data protection laws and regulations, as well as any safe harbor and contractual requirements adopted by the company.

Endnotes

1 Although employers that do not provide health services are not generally covered by the HIPAA rules, they may nevertheless be subject to the act's restrictions in their capacity as administrators of a health plan.

2 Forty-nine U.S. states and territories have enacted data breach notification laws in some form.

3 Safe harbor certification is also available under Swiss data privacy law, which is similar to the EU directive.

4 The U.S. Department of Health and Human Services has investigated and resolved thousands of HIPAA data security incidents and complaints, but the agency imposed its first-ever civil monetary penalty for a HIPAA privacy rule violation in February 2011, in the amount of $4.3 million (the majority of which was attributable to the entity's failure to cooperate with the agency's investigation).

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | 1.877.323.4171

Pillsbury Winthrop Shaw Pittman LLP