By J. C. Bruno and Elsa Crozatier

Compliance with the European Union Directive in the Transfer of Employee Personal Data to U.S. Affiliates

U.S. companies with parents, subsidiaries, affiliates, customers, or business partners in the European Economic Area should be concerned about compliance with European law regulating the sharing of employee data.

The European Parliament has adopted a directive to protect European personal data, which went into effect in 1998 (Directive).[1] It requires Member States to enact laws protecting the process of personal data in the European Union (E.U.) and prohibiting the transfer of personal data to countries outside the E.U. (Third Countries) that fail to ensure the European "adequate level of protection." The Directive has been implemented by legislation in E.U. countries and in the European Economic Area (E.E.A.).[2]

The data exporter (e.g., a European subsidiary), and in some cases, the data importer (e.g., a U.S. parent), can be subject to sanctions for violation of an E.E.A law. Each E.E.A. Member State has its own sanctions for violation of the national legislation. In Spain, the fine can reach 600,000 Euros; in Germany, a company can be charged with administrative or criminal offenses punishable by a fine of up to 250,000 Euros. Furthermore, a possible penalty under all national legislation is a prohibition of the transfer of personal data. This sanction can be serious for a company, and country, that receives a significant amount of data from the E.E.A. Although enforcement seems to be sparse and monetary penalties may not be significant for large multinationals, many companies have complied with the Directive because of a risk of adverse publicity, which can create irreversible damage to a company's reputation and business. For example, DoubleClick lost billions of dollars because of accusations that it violated its stated privacy policies while tracking online consumers.[3]

Consequently, companies operating and processing personal data in the E.E.A., as well as companies established in a Third Country receiving personal data from E.E.A., must comply with E.E.A. legislation. This article explains the Directive, its scope, its requirements for Member States, and describes the methods of compliance available to U.S companies with their parents, subsidiaries, affiliates, customers, or business partners in E.E.A.

The Broad Scope of the Directive

The initial goals behind the Directive are understandable. The European Parliament wanted to harmonize E.U. national privacy laws and to ensure the free movement of personal data within the E.U. The Directive has been criticized, however, as an example of excessive government regulation.[4] The definitions stated by the Directive are very broad. Personal data includes any information relating to an identified or identifiable natural person. This has permitted the European authorities to interpret the Directive as including innocuous information such as an employee's office phone number in a worldwide company phone book. A separate status and more stringent protection has been provided for "sensitive data."[5] The classification of personal data as sensitive data is important because it is forbidden to process such data, even between E.E.A. countries, unless a specific exception applies. In the same way, the definition of processing and its interpretation are very broad. According to the Directive, any operation involving personal data, whether or not by automatic means, such as, the collection, recording, filing, storage, use, and the disclosure by transmission, is considered processing.

Consequently, the scope of the Directive is very broad as to all personal data, with its most strict provisions applying to sensitive data. Member States are required to enact laws following the provisions of the Directive to protect personal information.

The Requirements to Member States' Legislation

The Directive requires Member States to enact legislation to provide various types of protection for personal data processed within

"Business Problems and Planning" is a department of the *Michigan Bar Journal*. The editor is J. C. Bruno of Butzel Long, Ste. 900, 150 W. Jefferson, Detroit 48226.

The editor invites lawyers and judges to submit articles to be considered for publication. Articles should focus on planning opportunities and on practical solutions to common problems encountered in representing businesses. They should be short, practical, and under 1,250 words.

the E.E.A. These principles, often closely related to each other, are cumulative and can be summarized as follows:[6] legitimacy; finality; proportionality; retention; security; accuracy; data subject's rights; notification to the data protection authority (DPA).[7] Companies processing personal information within E.E.A. must comply with the Directive and the national legislation. Care should be taken with sensitive data because, as described above, special provisions apply to its processing.

The Directive also requires Member States to enact laws prohibiting the transfer of personal data from an E.U. country to a Third Country that does not ensure the European "adequate level" of protection, unless one of the limited exceptions applies. Presently, only four countries, Switzerland, Canada, Guernsey, and Argentina,[8] have enacted laws considered adequate by the E.U. Commission. The United States is not considered as ensuring an adequate level of protection. In July 2000, the U.S. Department of Commerce (DoC) concluded negotiations with the E.U. Commission for adoption of a Safe Harbor Principles Framework (Safe Harbor Principles).[9] Under the Safe Harbor Principles, it is the U.S. company that self-certifies adherence to the Safe Harbor Principles that is deemed to provide an adequate level of protection. Besides the Safe Harbor Principles, there are other options available to a U.S. company to comply with the Directive.

The Compliance Solutions Available to U.S. Companies

The transfer of personal data from E.E.A. to the U.S. is allowed only if U.S. companies ensure an adequate level of protection by either falling within one of the exceptions stated by the Directive[10] or by self-certificating under the Safe Harbor Principles. Some of these exceptions are discussed below.

An Overview of the Most Valuable Exceptions Provided by the Directive

The data subject's unambiguous consent. A company using this exception must know if the transfer requires an opt-in or an opt-out consent.[11] For sensitive data, the Directive requires opt-in consent, while for non-sensitive data it permits opt-out consent. However, some E.U. countries, such as Portugal, require opt-in consent for all personal data. Moreover, there is a general suspicion in the E.U. as to whether the consent can be freely given in the employment context. The E.U. has discussed the possibility of a new directive eliminating consent in employment relationship, but it has not been introduced yet. It is likely that the consent exception will disappear in the employment context. The only question is when.

The contractual solution. A company based in a Third Country can enter into a contract with the data exporter established in an E.E.A. country to provide the required adequate level of data protection. It must be either an individually negotiated contract (Ad Hoc Contract) or a contract incorporating the standard contractual clauses that have been approved by the E.U. Commission (Standard Contractual Clauses).[12] Unlike the E.U. Standard Contractual Clauses, an Ad Hoc Contract has to be approved by the DPA of each country from which personal data will be transferred. This article only discusses the Standard Contractual Clauses.

The Standard Contractual Clauses are not a very attractive solution.[13] If a national law requires it, the parties must deposit a copy of the contract with the DPA and its approval must be obtained. Moreover, enforcement can have serious repercussions for the data importer. Data subjects can enforce the contract as third-party beneficiaries and sue either the data importer or data exporter. Both are jointly and severally liable for any damages. The Standard Contractual Clauses also provide for jurisdiction courts setting in the E.E.A. and that the law governing the contract must be the law of the Member State where the data exporter is established (e.g., the law of an E.E.A. country).

The code of conduct. This exception may have future value.[14] It could be of interest to a multinational because it would allow the transfer of personal data among different entities within a control group. However, until now, this solution has been interpreted strictly and it is currently not a practical alternative. In fact, a code of conduct must be approved by the DPA of each country in which the company operates and each DPA

has authority to require modifications, which make the process lengthy and tedious. Consequently, companies are reluctant to opt for this exception and only a few codes of conduct have been put into place (e.g., Daimler-Chrysler Code, FEDMA Code).

Most U.S. companies use neither the contractual nor the code of conduct exception. They opt for an alternative solution, consent and/or the self-certification to the Safe Harbor Principles, but even this alternative has its limitations.

The Safe Harbor Principles, the U.S. Patch

As previously discussed, the United States is not considered as ensuring an adequate level of protection. The Safe Harbor was negotiated as a patch for U.S. companies. All Member States are bound by the adequacy determination.[15] As a voluntary system, it applies only to U.S. companies that subscribe to it. The registrant (harborite) can limit the self-certification to certain categories of data. They were 500 harborites in May 27, 2004, such as General Motors, Microsoft, Procter & Gamble, Oracle, IBM, Marriott International, Pepsi, Ernst & Young, and Intel. Before submitting the self-certification form to the DoC, the company must:

1. Confirm that the organization is subject to the jurisdiction of either the Federal Trade Commission or the Department of Transportation;
2. Select an appropriate officer, generally a "Privacy Officer," as a central contact person and prepare a statement of his/her responsibilities;
3. Develop and implement a Privacy Policy Statement (Policy), which must be compliant with the FAQ and the seven Safe Harbor Principles.[16]

To protect employees, the Safe Harbor Principles and especially FAQ 9 contain specific provisions for the processing of human resources data. For such data, the harborite must comply with national requirements for processing and the transfer of personal information, even after the initial transfer. The enforcement Principle is more strict too. Moreover, the company has no choice and must agree to cooperate with the competent DPA for human resources data. Cooperation may mean compliance with investigations and decisions. Lastly, FAQ 9 states that, "in the context of employment relationship, primary responsibility for the data vis-à-vis the employee remains with the company in the E.U." Consequently, in the employment context, it seems to be the jurisdiction and the law of the data exporter that applies, while data collected outside the employment context, it is U.S. law and jurisdiction that apply.

How to Choose between the Exceptions Stated by the Directive and the Safe Harbor Principles?

The Safe Harbor Principles and the exceptions stated by the Directive are alternative and thus, not cumulative. However, it can be interesting for some companies to opt for a combination of them. Companies should avoid the consent exception or at least, use it as a last resort, because there is a risk of refusal by the data subject. U.S. companies should opt for the Safe Harbor Principles for non-human resources data and should require data subject consent for such data.

At least four arguments are in favor of the Safe Harbor Principles for non-human resources data. First, the harborites are listed on the website of the DoC.[17] This may have a positive effect on public, employee, and customer relations. Second, the form of the Safe Harbor Principles corresponds more to the American point of view of privacy protection. The contractual solution requires much more information than the Safe Harbor Principles. Third, the law governing the Safe Harbor Principles is U.S. state law, while the Standard Contractual Clauses must be governed by the law of the Member State of the data exporter. Fourth, because all Member States are bound by the adequacy determination,[18] a harborite satisfies the law of all E.E.A. countries. With the contractual solution, the U.S. company would have to make contracts with every company in E.E.A. with which it wants to transfer personal data. Consequently, U.S. companies should generally opt for the Safe Harbor Principles, at least for data other than human resources data.

Some of the advantages of the Safe Harbor Principles do not apply in the employment context. As stated above, the Principles are more strict for human resources data, which reduces, or perhaps eliminates, the benefits of the Safe Harbor Principles. For example, for employee data, the law governing the Safe Harbor Principles is the E.E.A. national legislation, the jurisdiction is the jurisdiction of the data exporter, and lastly, the harborite must comply with national E.E.A. legislation and thus, provide further requirements for human resources data. As a result, U.S. companies may not opt for the Safe Harbor Principles in employment relationship but for an alternative solution, which is either the Standard Contractual Clauses or the data subject consent. Care should be taken with the consent because opt-in consent is required in some E.E.A. countries for processing and because this exception may disappear soon for human resources data. However, currently, U.S. companies seeking to comply with the Directive often opt for the data subject's consent for human resources data.

U.S. companies may opt for a combination of the solutions, the Safe Harbor Principles in employment relationship and an alternative solution in such context. General Motors, for example, has only self-certified for a very narrow category of data and requires the consent for some others.

Conclusion

Most U.S. companies continue to be skeptical about the need for compliance with the Directive. Despite this lack of concern about legal penalties, U.S. companies should comply with the Directive to avoid the possibility of sanctions, embarrassing private litigation, and adverse publicity. It is also good business to comply with the legitimate privacy concerns of suppliers, customers, and employees. Companies should audit and revise their policies and practices, train employees in the proper handling of personal data, establish a strong "Privacy Officer," and develop awareness of and compliance with privacy rules. Consumers care about the protection of their personal data. Publicity over a privacy violation could have irreversible repercussions on business. Compliance with privacy regulations is not only a legal issue, it is also a business requirement. ✦

J. C. Bruno is a shareholder of Butzel Long, P.C. and practices transactional and corporation law.

Elsa Crozatierhas passed the Paris bar exam and has completed a legal internship with Butzel Long P.C.

FOOTNOTES

1. The Directive "On the protection of individuals with regard to the processing of personal data and on the free movement of such data" is available at http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.
2. A directive does not have the effect of a law. Each E.U. Member States must enact national laws meeting, at least, the basic standards of the directive. It is the national law that applies then. As of May 1, 2004, the E.U. includes 25 countries. Presently, the 15 countries of the old E.U. have implemented the Directive except France, and Hungary is the only country of the new ten E.U. countries that has enacted a law deemed adequate. Any references to the E.U. in the Directive should be understood as referring to the territory of the E.E.A. (E.E.A. Joint Committee No 83/1999) The E.E.A. includes the E.U. countries plus Iceland, Norway and Liechtenstein.
3. http://www.deloitte.com/dtt/article/0,2297,cid=26769&pv=Y,00.html.
4. *Wall Street Journal*, Europe's New High-Tech Role: Playing Privacy Cop to the World, David Scheer, Friday, October 10, 2003.
5. Directive Art.8.
6. The eight principles are derived from Directive Arts. 6, 7, 10, 11, 12, 14, 15, 16 and 17.
7. A DPA is an independent supervisory authority established in each Member State (Directive Art. 28).
8. Their laws are available at http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm.
9. The Safe Harbor Principles Framework is set forth in a set of seven privacy principles, 15 FAQs, the E.U. Commission's adequacy decision, the exchange of letters between the DoC and the E.U. Commission, and letters from the DoT and FTC on their enforcement powers.
10. Directive Art. 26 and 27. It must be remembered that whatever the basis of the transfer to a Third Country, processing involved in the transfer must still satisfy the processing requirements stated above.
11. Opt-in consent is a consent affirmatively given by the data subject while opt-out consent only requires that the data subject is provided an opportunity to object to transfers. Opt-in consent can be a significant issue for the company if the data subject refuses to give it.
12. The E.U. Commission has published Standard Contractual Clauses for the transfer to data controllers and a draft to data processors.
13. The International Chamber of Commerce negotiated with the E.U. an alternative version of Standards Contracts Clauses which is more flexible. But it has not been approved yet.
14. Working Party 11639/02/EN WP 74.
15. E.U. Commission decision of the adequacy of the Safe Harbor Principles available at http://www.export.gov/safeharbor/DecisionSECGEN-EN.htm. Decision the E.E.A. regarding to the Safe Harbor Principles http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_045/l_04520010215en00470048.pdf.
16. The seven Principles are notice, choice, onward transfer, security, access, data integrity and enforcement. http://www.export.gov/safeharbor/sh_documents.html.
17. http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.
18. http://www.export.gov/safeharbor/DecisionSECGEN-EN.htm.