

Article from **INTERNATIONAL LEGAL NEWS** ([http://www.imakenews.com/iln/e\\_article000597712.cfm?x=b11,0,w](http://www.imakenews.com/iln/e_article000597712.cfm?x=b11,0,w))

June 7, 2006

## Do EU-Based Employees Have Extra Privacy Rights Over Their Personal Data?

Epstein Becker & Green, P.C., New York, USA

by A. Jonathan Trafimow

Multinational companies transferring employees from nations in the European Union to the United States must cope with legal restrictions on the transfer of their employees'

personal data into the United States. These restrictions are complex; for example, it can be hard even to determine which jurisdiction's privacy laws apply to a particular employee's information. How are employers supposed to abide by the law when it is complicated even to determine what the law is?

To understand the issue, it is necessary to outline the differences in the ways these two economic powers perceive privacy. The United States, in valuing the individual's right to keep personal details private, has adopted a piecemeal approach to privacy protection. Each sector, it seems, addresses the issue its own way. In the health-care industry, for example, patient privacy is governed by HIPAA, while the human resources professional is typically concerned with the ADA and its nondisclosure of confidential medical information requirements. State laws often add to this mosaic, as is seen in a December 2005 New York law that requires employers in that state to notify their employees who live in that state if their personal data is compromised due to a breach in computer security.

The European approach is philosophically different. In the European Union, a person's right to privacy in personal data is viewed as a *fundamental* human right. The European Union, therefore, has adopted a comprehensive legislative framework intended to protect this data from broad disclosure. This legislation, called the "European Data Protection Directive" (the "Directive"), regulates information privacy across sectors.



EPSTEIN BECKER & GREEN P.C.



EBG

## **The Directive's Protections**

The Directive restricts the “processing” of “personal data.” Both “processing” and “personal data” are broadly defined terms.

- “Personal data” means “any information relating to an identified or identifiable natural person.” “Identifiable person” is defined broadly as someone “who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”
- “Processing” means “any operation or set of operations which is performed upon personal data.” Some examples listed in the Directive are “collection,” “storage,” “retrieval,” “consultation,” “dissemination or otherwise making available” and even “erasure.”

As a result, the Directive restricts a wide range of activities that employers might otherwise perform on various types of personal data. For example, an employee’s personnel file will probably fall under the definition of “personal data,” and the transmittal thereof may constitute “processing.” This broad definition makes any attempt to definitively list those documents that would constitute “personal data” problematic.

The Directive requires Member States (that is, European Union members) to protect personal data that is to be transferred to non-European Union nations. Member State organizations may only transfer personal data if persons receiving the data reside in a nation that legally requires an adequate level of protection, or, if the transferee nation does not meet the standards, the Member State must ensure that certain conditions are met. The European Union does not consider U.S. privacy laws adequate to protect interests that, as noted, the European Union considers to be a fundamental human right.

## **Potential for Liability**

With U.S. law not up to European Union standards, a multinational employer could not transfer an employee’s personal data from a Member State to the United States without running the risk of liability. Articles 22 through 24 of the Directive require Member States to employ a judicial framework, allowing the aggrieved individuals a remedy for any breach of the Directive, including compensatory damages and other state-imposed sanctions.

In addition to liability, employers need to appreciate the procedural morass that personal data transfer litigation might entail. Personal data can flow freely between European Union Member States and, as employees move throughout the European Union, is increasingly likely to do so. Further, each Member State will have its own Directive-compliant data protections law. Imagine the procedural quagmire that might occur if an employee with prior duties in London, Paris, and Hamburg is transferred to Chicago – along with his personal data. The corporation could be sued for the allegedly unlawful transfer of personal data under British, French, and German law. All three nations, plus the United States, could have jurisdiction over the matter.

## **The Safe Harbor**

The philosophical and legal issues noted above had the potential to lead to significant economic and diplomatic friction. These potential difficulties were averted through two years of negotiation between the U.S. Department of Commerce (“DOC”) and its European Union equivalent.

As a result, the U.S. Commerce Department adopted the “Safe Harbor Privacy Principles,” since acknowledged by the European Union, which set forth, among other things: (i) the scope of the United States’ privacy principles; (ii) the requirements that U.S. organizations must meet in order to enter the Safe Harbor; and (iii) the procedures for enforcing the Safe Harbor.

American companies transferring an employee from an EU Member State to the U.S. should understand the Safe Harbor, how to use its procedures to lawfully accomplish transfers of European Union employees to the United States, and the advantages and disadvantages of various legal options available to them. Employers may have to change their internal recordkeeping policies and procedures to comply with the Safe Harbor requirements.

To participate in the Safe Harbor, an American company must self-certify to the DOC that it adheres to the Safe Harbor requirements. The certifying organization must notify individuals that their information may be collected and used, and for what purpose. Further, the organization must allow these individuals to withhold consent for their information to be shared with a third party, and must allow individuals to access their personal information. The organization must also prevent data loss and the misuse, accidental disclosure, and loss of data integrity. The organization must further take reasonable steps to ensure that all privacy protections travel with the data, such as verifying that the transferee company has agreed to abide by the terms of the Safe Harbor. If the transferring company fails to do so, it may be open to civil liability.

Enforcement of these provisions occurs in a roundabout way. Companies that certify their compliance with the Safe Harbor guidelines by this very act publicly represent that they will adhere to the guidelines set forth by the regulators. Indeed, the U.S. Commerce Department maintains a list of those companies that have certified that they comply with the Safe Harbor’s requirements. This list is readily available on the Department’s website at <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>. As of April 24, 2006, that page, in bold letters, announced that the organization’s inclusion on the list “constitute[s] a representation to the Department of Commerce and the public” that the company complies with the Safe Harbor framework.

## Liability Under the Safe Harbor

During the time period of avowed compliance, this public declaration has legal consequences. Section 5 of the Federal Trade Commission Act empowers the Federal Trade Commission to bring actions against those organizations that make misrepresentations to the public. (Not all organizations are regulated by the FTC. For example, many banks and insurance companies are not.) For example, a company that certifies compliance with the Safe Harbor but is not *actually* compliant would, in fact, be making such a misrepresentation. Therefore, the Federal Trade Commission may sue any company in its regulatory jurisdiction that claims to follow the Safe Harbor provisions but fails to actually do so, much as it could bring an action against a corporation for false advertising.

Certification, however, is not a promise to abide by the terms of the Safe Harbor *ad infinitum*. An organization may withdraw from the program in two ways. First, the passive method: notification of compliance is only valid for twelve months, and organizations must, in the Commerce Department's words, "reaffirm their continued adherence to the Safe Harbor framework" every year. Similarly, there is an active escape: a company may withdraw at any time, relieving itself of any obligations to abide by the provisions of the Safe Harbor agreement going forward, by notifying the Commerce Department of its intent to withdraw. Those organizations that do *not* opt in to the Safe Harbor (or that do opt in, but withdraw) risk violating the European Union's Directive if a European Union employee's data is transferred to the United States.

A person who believes his data was mishandled by a Safe Harbor participant may also complain to the European Union. As part of the Safe Harbor, the European Union has set up a "data protection panel" authorized to investigate complaints of individuals who believe their data has been compromised by a breach of the Safe Harbor provisions. (The panel only has the authority to investigate the alleged transfer of certain types of personal data; for other types of personal data, the panel has no investigative authority unless the company has agreed to use the panel as an independent recourse mechanism. Companies that have not agreed to use the panel for this purpose will usually employ some sort of private dispute resolution system. Frequent web surfers may be familiar with some of these services, such as TRUSTe, that help ensure the protection of sensitive data transmitted in e-commerce transactions.)

The panel, upon finding that the principles of the Safe Harbor were violated, will make recommendations to the alleged violator in hopes of rectification. If these suggestions go unanswered, the panel may opt to refer the matter to the Federal Trade Commission, underscoring the international cooperation involved throughout the Safe Harbor process.

## Other Alternatives

Self-certification under the Safe Harbor is not the only way for an employer to potentially avoid liability under the European Union Directive. For specific transfers, transferor and transferee may enter into an explicit contract, which will require the approval of relevant authorities. An agreement that is intended to apply more broadly can rely on language adopted by the European Union. Templates are available at [http://europa.eu.int/comm/justice\\_home/fsj/privacy/modelcontracts/index\\_en.htm](http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm). According to the Directive's regulatory gloss (such as administrative decisions and opinion letters), adherence to these models typically does not require prior approval from the relevant authorities.

Similarly, a multinational employer may be able to comply with the European Union's rules by adopting a set of binding corporate rules that regulate the flow of personal information and do so

with the approval of relevant European Union authorities. This method is both new and untested, and it remains unclear whether it will be an effective approach to an already murky problem. However, the approach has received a green light from a European Union advisory board and has already been put into effect by several multinational corporations. Binding rules may become the gold standard for Directive compliance, but at this early stage it is still unclear whether this route will survive the scrutiny of all the nations subject to the European Union Directive.

## Employer Options

How to comply with the Safe Harbor is a decision each organization must make individually. Not opting in to the Safe Harbor can subject an employer to substantive and procedural legal complexities; however, agreeing to partake in the program also has significant legal consequences. Multinational employers must be aware that both the United States *and* the European Union may independently regulate any EU-to-U.S. transactions of personal data by organizations that adopt the Safe Harbor. And, finally, the organizations should be aware of other methods to ensure compliance with the various laws out there.

*A. Jonathan Trafimow is a Member of the firm in the New York office of Epstein Becker & Green, P.C., a general practice law firm with over 380 attorneys practicing in 11 offices throughout the United States and with affiliations worldwide. Please feel free to contact Mr. Trafimow at (212) 351-4573 or [jtrafimow@ebgLaw.com](mailto:jtrafimow@ebgLaw.com) with any questions or comments about this article or other related issues..*

*The author wishes to thank Daniel N. Lewis and Francesca Fleuri for their contributions to this article.*

*This document has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.*

© 2006 Epstein Becker & Green, P.C.

Published by [Alan Griffiths](#)  
Copyright © 2008 International Lawyers Network. All rights reserved.

Powered by [IMN](#)