# The Next Great Trans-Atlantic Voyage

European laws protecting human resources data arrive on America's shores


Shanti Atkins, Esq.
Philip L. Gordon, Esq.
Scott J. Wenner, Esq.

LITTLER MENDELSON®
A PROFESSIONAL CORPORATION
THE NATIONAL EMPLOYMENT & LABOR LAW FIRM®

Gary Clayton
PRIVACY COUNCIL℠

# The Next Great Trans-Atlantic Voyage:

## European Laws Protecting Human Resources Data Arrive on America's Shores

## Introduction

Globalization! The much-ballyhooed war cry of American business during the past decade could soon become a double-edged sword for United States businesses with employees in the European Union (the "EU"). The EU's fifteen[1] Member States have slowly commenced enforcement of, or will soon begin to enforce, unprecedented privacy-based restrictions on the "export" to the United States of "personal data" concerning EU residents. These new barriers, raised in consequence of the EU's Data Protection Directive (the "EU Directive"), affect far more than the well-publicized transfers of customer information generated by businesses engaging in e-commerce. Virtually every transfer of human resources data from operations, affiliates, or subsidiaries in the EU to United States headquarters or business units—even a transfer of basic personnel information such as an employee's name, work address, and work telephone number—is subject to these restrictions and triggers broad obligations.

Given the imminent enforcement of European laws regulating the transfer of data from the EU to the U.S., in-house counsel and human resources professionals at U.S. corporations with employees in the EU must assess, if they have not done so already, whether, and how, to put their company's information-handling practices in line with the EU's data protection standards. Compliance will require many corporations to radically change how they collect, store, use, transfer and disclose—i.e., "process"—their human resources data. This is because what many human resources professionals in the United States would consider to be "business-as-usual" data handling practices are patently illegal under data protection laws in Europe where privacy is considered a fundamental human right. That, in turn, places both the European transferor and the U.S. transferee at risk.

It is reasonable for members of the legal and human resources departments to ask why they should prevail upon their companies' business units to commit scarce capital, time, and attention to an effort that might appear quixotic in the context of the United States business culture. The answer: non-compliance with European data protection laws is a smoldering ember which, if left unattended, could suddenly engulf your company in a conflagration of bad publicity, civil lawsuits, government enforcement actions, loss of important data, and internal recriminations.

While the European enforcement record remains relatively undeveloped at this early stage, authorities in EU Member

[1] The present number of members is certain to grow in this decade as nations, many formerly in the Eastern Bloc, who were unable to satisfy the rigorous admission standards earlier, vie for admission.

States have been authorized to levy corporate fines ranging from small amounts per offense to close to $600,000 per offense (in Spain).[2] Not only are some corporate employees financially at risk, but they and their employers also could face criminal prosecution (in Italy[3] and in the United Kingdom,[4] for example), with convictions for particularly egregious violations resulting in imprisonment. Perhaps even worse for the corporation, an offending business could be barred from eligibility to receive and use personal data coming from Europe, and could be ordered to destroy any such data that it acquired unlawfully. Finally, the bad publicity associated with these enforcement actions could seriously tarnish a corporation's hard-earned public image. Put simply, no U.S. corporation can afford to ignore the EU's data protection regime.

This paper will address the practical impact of the EU Directive on human resources management at U.S. companies with European operations. We also will explain the three most practical options that in-house counsel and human resources professionals should consider as they develop strategies to help guide their business through uncharted terrain. In the end, this paper should equip the reader with a basic understanding of how the data protection laws now directly applicable to their corporation's European operations will demand new approaches to the collection, storage, use, and disclosure of human resources data at United States headquarters as well as in Europe, and the options for addressing this change.

## HOW THE EU DIRECTIVE AFFECTS YOUR HUMAN RESOURCES FUNCTIONS

### *The Basic Principles Of The EU Directive*

The EU Directive, which was enacted in 1995, required the fifteen EU Member States to implement national data protection laws by 1998. The Directive established minimum standards for these national laws. However, the Directive's standards are broadly written, leaving room for interpretation and interstitial legislation by each Member State to fit its own social and political culture and its national experience. As a result, strong common threads will be seen running through the data protection laws of all EU Member States, but there are also important distinctions from country to country. United States in-house counsel and human resources professionals advising a company with employees in, for example, the United Kingdom, Belgium, and Spain must be prepared to encounter three separate, but related, sets of data protection laws administered in those nations by different administrators and through differing procedures.

To communicate effectively with European counterparts and European data protection authorities, human resources professionals in the U.S. and their legal advisors must become familiar with the Directive's data protection lexicon. The key terms most foreign to United States notions of privacy law are defined below:

- PERSONAL DATA: any information relating to an identified or identifiable natural person;
- SENSITIVE PERSONAL DATA: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, or sex life;
- DATA SUBJECT: the natural person to whom personal data relates;
- PROCESSING OF PERSONAL DATA: any operation, or set of operations, performed on personal data, whether or not by automated means (such as collection, recording, organization, storage, transfer, alteration, retrieval, use, or disclosure);
- DATA CONTROLLER: the person or entity who alone, or jointly with others, determines how, and for what purpose, personal data will be processed;
- DATA PROTECTION AUTHORITY: the national regulatory agency responsible for ensuring that data collectors comply with national data protection laws.

The EU Directive requires enactment of national laws throughout the EU that establish strict limits on the processing of personal data, impose significant obligations on the data controller vis-à-vis the data subject, and confer substantial rights on the data subject vis-à-vis the data con-

[2] *See* Organic Law of 13 December 1999 on the Protection of Personal Data, Art. 44(4)(a).

[3] *See* Act No. 675 of 31.12.1996 (consolidated), Chapter VII, Article 35.

[4] *See, e.g.*, Data Protection Act 1998, ch. 2, §§21m 47(1).

troller. As applied to the employment context, the Directive's chief principles guiding the application of data protection laws include the following:

- LEGITIMACY: The employer (the "data controller") may process an employee's (the "data subject's") personal data only (a) with the employee's prior consent, (b) as necessary to perform the employment contract, or (c) to the extent necessary to comply with legal obligations;
- NOTICE: Before processing personal data, the employer must inform the employee of the personal data being collected, how and why the personal data has been or will be processed, to whom the data has been or will be disclosed, and whether the data will be exported outside the EU or to a country which does not provide "adequate" protection;
- PROPORTIONALITY: The employer may process data for the purpose disclosed to the employees, or for a compatible purpose, but in all events the personal data which is processed must be the minimum necessary to carry out that purpose. It would violate the "minimum necessary" requirement, for example, to require a job applicant to provide the European equivalent of a social security number if that number will not be used in connection with the hiring process;
- ACCESS: The employer must (a) grant each employee's reasonable request for access to the personal data it maintains; (b) provide each employee with the opportunity to correct, erase, or block further processing or transfers of inaccurate, outdated, or incomplete data; and (c) notify any third party to whom inaccurate, outdated, or incomplete data has been disclosed of any additions or corrections made in response;
- SECURITY: The employer must protect the data from unauthorized access and disclosure;
- TRAINING: The employer must train employees, as appropriate, in applicable data protection requirements.

The precise application of these abstract concepts to the day-to-day human resources functions of a business enterprise employing dozens, or thousands, of employees is a complex matter still being debated at the EU's highest levels and refined at the national level. What is clear, however, is that the national laws implementing the Directive's broad principles will apply to and generally limit the collection, storage, transfer, use, and disclosure of a wide range of human resources data which, in the United States, would be considered freely subject to use and disclosure wholly at the discretion of the employer.[5] For example, national data protection laws of EU members will govern, for employees residing in that state, the processing of resumes, job applications, sickness and leave records, performance evaluations, and even employee contact information within the organization.

While compliance with the national data protection laws implementing the EU Directive most likely will fall primarily within the purview of your European counterparts and advisors, the EU Directive, nonetheless, demands that you understand what your company must do to comply with those laws and how the data protection authorities where your company has European operations are administering and enforcing those laws. These matters cannot simply be left on the other side of the Atlantic because, as noted above, European data protection authorities have the power not only to levy substantial fines on violators, but also to block transfers of personal data from your European operations. Furthermore, the national laws will govern how data may be processed in Europe before it is transferred to the United States, and thus will determine whether certain data may be transferred at all. And finally, under certain circumstances (described below), your U.S. organization may have to pledge to cooperate with the data protection authority of each EU member from whose country data is exported. These authorities and the laws they administer matter to U.S. corporations doing business in Europe.

### *The Extra-Territorial Reach Of The EU Directive*

Central to the EU Directive is a general prohibition against the "export" of personal data to any country not providing privacy protections deemed adequate under EU standards. The national data protection authority can easily enforce this prohibition because under the EU Directive, the nation-

[5] There are exceptions to this proposition at the state level in jurisdictions such as California, which recognize a state constitutional right to privacy that has been held to be applicable to private employment relationships. This is a distinct minority view in the United States, however. More states, *e.g.*, New York, are at the opposite end of the spectrum, essentially recognizing only a very limited right of privacy in the commercial context.

al laws of each Member State must require that a data controller seek and obtain approval from the national data protection authority before "exporting" personal data to a non-EU country. Circumventing EU data protection authorities could have the severe administrative, financial, and even criminal repercussions described above.

Proud as Americans are of their legal system, the EU has determined that the laws of the United States do not adequately protect personal data.[6] Consequently, when your European counterparts or advisors apply to the appropriate national data protection authority for approval to send even the most basic human resources data to the United States home office, they will bear the burden of demonstrating that one of the exceptions to the general prohibition against exporting human resources data to the United States applies. We discuss below the principal exceptions to the prohibition of data transfers from the EU to the U.S.

## AVOIDING DISRUPTION OF YOUR HUMAN RESOURCES FUNCTIONS—THE OPTIONS FOR MAINTAINING THE FLOW OF DATA

The current regulatory regime offers three principal options for the management of human resources data by United States corporations with employees in an EU Member State: (1) re-direct transborder data flows to avoid national data protections authorities; (2) certify compliance with the "Safe Harbor Principles" negotiated by the U.S. Department of Commerce; or (3) provide contractual guarantees of adequate privacy protection. Deciding which option best suits your organization will depend upon a host of factors, including the data-processing methods of your European operations, the structure of your company's human resources management, the flow of human resources information within your organization, and the enforcement perspective of the applicable national data protection authority. We provide a brief overview of each option to assist you in developing strategies to navigate through the new regulatory environment.

### OPTION ONE: *Redirecting Transborder Data Flows*

Those United States corporations with employees in Europe having decentralized human resources management may be able to avoid the direct effect of the EU Directive on their United States operations altogether by processing human resources data related to EU residents only within the EU. By way of illustration, a United States company with employees in Amsterdam, Brussels, and London could centralize all human resources functions for those employees in Brussels. By taking the United States headquarters out of the human resources data flow, the corporation would avoid the need to adjust its privacy practices in the United States to meet European standards.

In reality, few U.S. corporations with employees in Europe could take advantage of this option. Because national data protection laws apply to personal data related to all EU residents, regardless of nationality, all human resources data related to United States citizens working in the corporation's European facilities would have to remain in Europe. United States executives would have to travel to Europe to participate in employment decisions requiring their review of performance evaluations of an employee in a European facility. As a third example, the corporation could not transfer to the United States any human resources information related to a European employee temporarily transferred to the United States.

In each of these situations, the United States corporation, in theory, could seek approval for each specific data transfer on an as-needed basis by demonstrating to the national data protection authority the applicability of one of the exceptions to the general prohibition against personal data exports to the United States. However, reliance upon these exceptions most likely would be both impractical and risky in view of the consequences.[7]

As one exception, the EU Directive permits EU Member States to allow transborder data flows to a third country not providing adequate privacy protections, like the United States, where the data subject consents to the data transfer.

[6] One need look no further than the European totalitarian regimes of the last half-century and the secret police under Hitler, in East Germany, and throughout the former Eastern Bloc to begin to comprehend the passion for personal privacy that is behind the EU Directive. The United States has nothing within its national experience to compare to the denial of the most basic personal privacy rights endured in wartime Europe and perpetuated during the Cold War.

[7] In addition, the notion that a U.S. company's human resources organization could avoid contact with personal data from the EU completely is even less reasonable when it is realized that any personal data, including data developed for *inter alia* sales and marketing purposes, could trigger application of the EU data protection mandates for the data transferred.

However, that consent, to be effective, must be "freely given." In the employment context, consent can be freely given only if (1) the employee receives prior notice of the purpose for the data transfer, and (2) the denial, or subsequent withdrawal, of consent would have no negative ramifications for the data subject. Thus, an employee would have unfettered power to veto a data transfer intended to permit United States executives to consider his demotion or discharge. Aside from this practical obstacle to relying upon consent, EU authorities responsible for interpreting the EU Directive have specifically warned employers *not* to rely upon employee consent when seeking permission to transfer human resources data to a third country lacking adequate privacy protections, both because of the ease with which consent can be revoked and because of the strict standards applied. Furthermore, in some EU Member States, such as Belgium, there are categories of data that employees may not consent to having transferred outside the EU. Any such consent is deemed void, thus leaving that transfer unprotected. In other EU countries, such as Germany and Austria, individual employees cannot consent on their own behalf; rather, the consent must be obtained through the employee, and some councils have taken the position that employees can not freely consent to the export of their personal data to the U.S. under any circumstances.

The EU Directive also permits Member States to allow data transfers to an "inadequate" third country where the transfer (a) is necessary to perform a contract between the data controller and the data subject, (b) is necessary to perform a contract between the data controller and a third party for the data subject's benefit, or (c) is legally required. These exceptions would cover, for example, the transmission of payroll information about a U.S. citizen employed in Frankfurt to permit U.S. headquarters to cut a paycheck, to pay insurance premiums on the employee's behalf, and to report to the Internal Revenue Service. However, the administrative delay inherent in first determining which exception applies and then in obtaining approval from national data protection authorities on a transfer-by-transfer basis could be extremely disruptive of such routine functions.

### OPTION TWO: *Certifying Compliance With The Safe Harbor Principles*

Given the importance of the trade relationships between Member States and the United States, government officials on both sides of the Atlantic labored to develop a framework which would permit a more regularized flow of personal data between EU Member States and the United States than would be permitted by reliance solely upon the narrow exceptions described above. The end product of these efforts is a set of privacy protections known as the Safe Harbor Principles. National data protection authorities in the Member States will approve the export of personal data concerning EU residents to any United States business which properly certifies its compliance with the Safe Harbor Principles. In-house counsel and human resources professionals considering the Safe Harbor option must understand that there are burdens associated with the benefits of administrative regularity and predictability so that the decision whether to join the Safe Harbor must be thoroughly analyzed.

Not surprisingly, the Safe Harbor Principles mirror many of the core principles embedded into the EU Directive and, therefore, may be as foreign to United States professionals addressing workplace privacy issues as the terms "data controller" and "data protection authority." The key terms and broad outlines of the Safe Harbor Principles, as applied to the employment context, are described below:

- NOTICE: Employers must clearly and promptly advise employees of the purposes for the anticipated use and disclosure of each category of personal data collected, the types of third parties to whom the information will be disclosed, and the procedure for lodging complaints concerning alleged violations of the Safe Harbor Principles;
- CHOICE: For "sensitive" personal information (defined above), the employer must obtain the employee's affirmative consent before disclosing the information to a third party or using the information for a purpose which is incompatible with the purposes for which the employer told the employee the information had been collected.

For all other personal information, the employer must give the employee the opportunity to "opt out" of the use or disclosure;

- ONWARD TRANSFER PROCESS: The employer must comply with the notice and consent requirements described above before disclosing personal data to a non-agent. The employer may disclose personal data to an agent without notice or consent if the agent provides adequate privacy safeguards, for example, by the agent's own certification to the Safe Harbor Principles or by the agent's contractual agreement to abide by those principles;
- SECURITY: The employer must take reasonable precautions to protect personal data from loss, misuse, unauthorized access and disclosure, alteration, and destruction;
- DATA INTEGRITY: The employer must take reasonable steps to ensure that the data is relevant to its intended use, and is accurate, complete, and current;
- ACCESS: Upon request, the employer must disclose to the requesting employee personal information collected from or about that employee in an EU Member State and processed in the United States after transmission from Europe. The employer also must provide the employee with the opportunity to correct, amend, or delete inaccurate information. The employer must notify third parties to whom the data has been disclosed of the inaccuracies.
- ENFORCEMENT: The employer, through an identified corporate representative, must certify annually to the Department of Commerce that (a) it has implemented policies to enforce the Safe Harbor Principles, (b) it has trained its employees in those policies, (c) it provides an internal complaint procedure for resolving complaints of non-compliance, (d) it periodically audits compliance, and (e) it will cooperate with EU authorities investigating complaints of non-compliance and will comply with any recommended remedial action.

### *The Potential Burdens Of Safe Harbor Certification*

While in theory a corporation is required to apply the Safe Harbor Principles only to personal data received from an EU Member State, it would be difficult, in practice, to justify to a company's workforce the much greater privacy rights conferred upon employees residing in Europe, particularly if those employees are United States citizens. Moreover, it may become impracticable to quarantine the personal data to which the Principles must be applied from that which is generated in the U.S. or elsewhere outside the EU, risking confusion between "protected" and "unprotected" data. Thus, as a practical matter, compliance with the Safe Harbor Principles may require a complete overhaul of your company's information-handling practices for your entire workforce.

An increased compliance burden is not the only potential cost of certifying to the Safe Harbor Principles. Although certification is purely voluntary, once a corporation certifies compliance to the Department of Commerce, the organization's failure to live up to that representation in connection with human resources data could result in the company's facing litigation in Europe. As noted above (*see*, "Enforcement"), a company which certifies to the Safe Harbor Principles must agree to comply with any remedy imposed by European data protection authorities empowered to resolve employee complaints that a U.S. employer has violated the Safe Harbor Principles.[8]

Moreover, the Federal Trade Commission could seek administrative penalties for what would be deemed an unfair trade practice (and, in egregious cases, the FTC could request in addition that the company be criminally prosecuted for making false representations to the United States government.) Indeed, FTC Chairman Tim Muris announced in his first major public statement that, under his stewardship, the FTC will emphasize enforcement of existing privacy laws and, in particular, the Safe Harbor Principles. The FTC will not necessarily wait for a referral from European authorities. In the FTC's view, the agency has the power to prosecute domestic complaints of Safe Harbor violations without European authorities first attempting to resolve the complaint.

### *The Potential Benefits Of Certification*

On the other hand, there are definite benefits to certification beyond ensuring the predictability of data transfers—itself a huge benefit. Companies certifying compliance

[8] The situation is different if the company's violation of the Safe Harbor Principles relates to its handling of customer data, as opposed to human resources data. In such circumstances, the U.S. company would be subject to sanction only in the U.S. Thus, one of the major advantages of certifying to the Safe Harbor Principles with respect to the processing of customer data is not present when considering whether to certify with respect to the processing of human resources data. A U.S. company may elect to certify with respect to one category of data, but not the other.

with the Safe Harbor may earn a reputation for being privacy-friendly employers among highly prized technical employees, providing a competitive advantage when labor markets tighten. Companies on the Commerce Department's publicly available Safe Harbor list also may burnish their reputation for trustworthiness with online consumers and with the media. Finally, a growing number of countries, including Canada, Switzerland, Japan, Hungary, New Zealand, and Australia, are implementing data protection regimes modeled on the EU Directive, in part to ensure that the companies within their borders maintain their own flows of data from the EU. Certifying compliance with the Safe Harbor most likely would go a long way towards putting your company in compliance with the data protection laws in these countries. Finally, certification to the Safe Harbor Principles can only enhance the reputation of the certifying company in European jurisdictions where its reputation will be important—those where it has a corporate presence or markets its products.

### OPTION THREE: *Contractual Data Protection Safeguards*

The Safe Harbor is not the only option available to those United States corporations with employees in an EU Member State for which redirecting transborder data flows is not a practical solution. At least where a European facility, affiliate, or subsidiary is organized as a separate entity, the United States company can agree by contract to provide privacy protections for data transfers from Europe that the national data protection authority would deem adequate. For some corporations, these data transfer contracts may be preferable to certifying compliance with the Safe Harbor Principles. For corporations in the banking and telecommunications sectors which are specifically excluded from the Safe Harbor, agreement to "data transfer contracts" presently may be the only feasible alternative for obtaining quick and routine approval of data transfers to the United States.[9]

To facilitate the use of data transfer contracts, the EU has developed a standard contract for exports of personal data to countries, like the United States, which do not provide adequate privacy safeguards under the EU's standards. The contract requires the parties to identify the categories of personal data to be transferred, the data subject or categories of data subjects to which that personal data relates, the reason that the data transfer is necessary, and the persons or categories of persons to whom the data importer intends to disclose the imported data. Under these contracts, the data importer agrees that when it processes the transferred data, it will abide by data protection provisions similar to the Safe Harbor Principles. In addition, the contract confers on the data subject the right to enforce the contract's privacy provisions against both the data importer and the data exporter through mediation, arbitration, or litigation (at the data subject's discretion) in the location of the data exporter and subject to that state's laws.[10]

#### *Advantages of the Standard Contractual Provisions*

There are two principal advantages to using a data transfer contract instead of certifying to the Safe Harbor Principles. First, the limited scope of a contract may permit the U.S. corporation to avoid the expense and administrative burden of a complete overhaul of its information handling processes to comply with the Safe Harbor Principles. Under the contract option, the corporation must provide expanded privacy protections only for the specific data which are the subject of the contract and the company is not required to conduct periodic compliance audits, engage in routine training, or promulgate an entire set of privacy policies, all of which are contemplated when agreeing to the Safe Harbor Principles. Second, the contract option reduces litigation risks because no corporate executive is required to make a public representation concerning the corporation's privacy practices and because the enhanced data protection obligations are limited to the personal data transmitted pursuant to the contract.

Significantly, the corporation can obtain the benefits of the contract option without necessarily foregoing the predictability of data transfers through certification to the Safe Harbor Principles. National data protection authorities are required to permit data transfers made pursuant to the stan-

[9] As of this writing, Safe Harbor protection for financial services and telecommunications companies is under active consideration.

[10] The standard contract can be found at http://europa.eu.int/comm/internal_market/en/dataprot/news/1539en.pdf.

dard contractual provisions except where those authorities have reason to believe that the data importer has not, or will not, comply with the contract's data protection requirements. Thus, predictability is virtually assured. In addition, the contract is standard for all EU Member States so that a corporation can use the same contract to transfer the same type of personal data relating to its employees in any EU Member State.

*Disadvantages of the Standard Contractual Provisions*

The narrow scope of the data transfer contract has its disadvantages as well. A U.S. corporation which imports personal data about its customers, or a wide variety of human resources data about its employees, may be required to execute an unwieldy number of contracts to cover the entire spectrum of data categories. In addition, the contracts could hamstring a company that may wish to use the imported data for an unanticipated purpose. By its own terms, the standard contract permits the data importer to use the imported data only for the purpose specified in the contract when the transfer was made. Thus, use for another purpose would place the data importer in breach of contract.

The data subject has the unilateral right to choose whether to mediate a data protection dispute or to bring a civil action in the courts of the Member State in which the data exporter is established. If the data subject and data importer both agree, they also can refer the dispute to arbitration if the data importer is in a country, such as the U.S., that has ratified the New York Convention on enforcement of arbitration awards.

However, regardless of the forum selected (mediation/litigation) or agreed to (arbitration), the Standard Contract Clause commits the parties to resolve disputes according to the data protection laws of the data exporter's country. The right of data subjects to choose unilaterally to litigate in the data exporter's courts means that by signing the standard contract in order to receive a data transfer from a source in a Member State, the data importer has subjected itself to the laws and the courts of a Member State. By contrast, U.S. companies certifying to the Safe Harbor are subject to remedial action in Europe for an alleged privacy violation in the U.S. only if the alleged privacy violation involved human resources data.

## ACTION PLAN FOR COMPLIANCE

Choosing among the three options described above, and then implementing the option best suited for your business, will not be an easy task. To assist you in this endeavor, we list below a series of steps intended to help you down the path towards compliance.

### A. THE INITIAL INQUIRY

#### 1. Determine Whether Your Company Must Comply With National Laws Implementing The EU Directive.

The obvious starting point in developing an action plan for compliance is to determine whether your business needs to comply at all. To answer that question you must first examine the scope of your operations in each of the 15 EU Member States.[11] You also should consider the scope of your company's operations in countries which have adopted a data protection regime similar to that required by the EU Directive[12] and in each country whose application to join the EU is pending.[13] You will need to consult with counsel familiar with the national implementing legislation in these countries to determine whether the nature of your company's operations in that country subjects your company to national data protection requirements.

#### 2. Assess The Current Flows Of Personal Data.

Doing business in an EU Member State alone will not require that you implement one of the three compliance options described above. The critical inquiry requires an examination of the *flow* of personal data between your company's EU operations, subsidiaries or affiliates and the U.S. You will need to obtain a complete inventory of individual exchanges, or of categories of exchanges, of personal data. For each exchange, or category of exchanges, your company should measure the frequency, materiality, and urgency of the exchange, and the cost of eliminating the exchange.

[11] The fifteen EU Member States are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.
[12] These countries include Australia, Canada, Hong Kong, Japan, and Switzerland.
[13] The list of applicants for membership in the EU includes Bulgaria, Cyprus, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovenia, and Turkey.

**3. Select A Compliance Option.**

If exchanges of personal data do not occur at all, or if exchanges are only incidental to your business's overall operations, then you should consider whether "Option One: Redirecting Transborder Data Flows" makes sense for your organization. That is, you should assess whether your company can operate without exporting any personal data from your EU operations to the United States. If the exchanges of personal data are more frequent or more material to your company's operations, then you most likely will have to choose between "Option Two: Certifying Compliance With The Safe Harbor Principles" and "Option Three: Contractual Data Protection Safeguards." The choice between these two options will depend, in large part, upon the frequency, variety, materiality, and urgency of data transfers between the EU and the U.S. and the relative cost of implementing each option. The more frequent and varied is the exchange of personal data, the more sensible the blanket assurance provided by the Safe Harbor would appear to be.

## B. IMPLEMENTING OPTION ONE: RE-DIRECTING TRANSBORDER DATA FLOWS

**1. Remove Your U.S. Operations From Transborder Data Flows.**

You have decided to eliminate the exchange of personal data between your U.S. and EU operations because you have determined that the benefits of those exchanges do not justify the cost of providing adequate safeguards for personal data exported from the EU. Now your company will be required to put in place technical, physical, and administrative safeguards to prevent the transfer of personal data from the EU to the U.S. This task will require coordination among various departments of your company, including information technology, human resources, and legal. If your company is obtaining personal data from consumers, the marketing department and business executives should be involved as well. One person, or a coordinating group with an individual chair, should be ultimately responsible for determining the types of personal data which currently are exchanged between the EU and the U.S. and the circumstances in which such exchanges occur. That person should then oversee the establishment and implementation of policies and practices which will eliminate those transfers of personal data in the future. To raise awareness of, and sensitivity to, the issue the designated privacy official should take a top-down management approach by, *inter alia*, identifying for those employees who actually handle persona data those categories of information which can not be "exported" to the U.S. and explaining the reasons for this restriction. Otherwise, inadvertent (but, nonetheless, unlawful) data transfers could result from poor communication among front-line employees or a lack of basic knowledge about data protection requirements.

**2. Make Contingency Plans For When Your U.S. Operations Have A Need To Know.**

Even when it makes sense for your U.S. operations to be removed from the flow of personal data processed in the EU, there inevitably will be instances in which your U.S. managers will need access to personal data processed in the EU. The person responsible for building the "personal-data firewall" between the EU and the U.S. also should be responsible for developing a contingency plan to handle those situations where U.S. executives unexpectedly have a need to review personal data processed in the EU, for example, to make a personnel decision or to develop a new marketing strategy. The point person should become familiar with the processes and requirements for using a "data transfer" contract to effectuate an otherwise impermissible export of personal data. That person also should discuss with counsel in the pertinent EU Member State the exceptional circumstances under which national implementing laws would permit the export of personal data to a country, like the U.S., which does not provide adequate privacy protections.

**3. Monitor The Data Protection Firewall.**

Your company's institutional memory will be only as long as that of the employees who comprise its workforce. For this reason, the person responsible for implementing this option must ensure that appropriate personnel continue to monitor and enforce the data protection firewall. This undertaking most likely will require training new employees on the restrictions which your company has put in place to make sure that no unlawful exports of personal data to

the U.S. will occur. Creating a regularly updated procedure manual also is advisable.

### C. IMPLEMENTING OPTION TWO: CERTIFYING COMPLIANCE WITH THE SAFE HARBOR PRINCIPLES[14]

Certifying compliance with the Safe Harbor Principles is a potential, data-transfer solution for a wide variety of businesses. An obvious candidate is the U.S.-based, multinational corporation with employees in many of the 15 EU Member States which has centralized all human resources functions in the United States. However, smaller businesses could greatly benefit from certification as well—for example, a small U.S. publisher of specialty books sold over the Internet directly to customers in each of the 15 EU Member States.

If, like the businesses described above, your business relies upon frequent and varied exports of personal data from the EU, joining the Safe Harbor most likely would be the preferable option. In that case, you should consider undertaking the following critical tasks associated with Safe Harbor membership.

#### 1. Certify Adherence To The Safe Harbor Principles.

You can obtain all the materials necessary to certify adherence to the Safe Harbor Principles from the Department of Commerce's Web site (http://www.export.gov/safeharbor/). The Web site also provides access to a library of explanatory materials. Much of this material has been prepared for non-lawyers. Nonetheless, given the significant implications attendant to certification, you should consult with counsel before submitting your company's certification to the Commerce Department.

#### 2. Conduct A Personal Data Audit.

Central to the task of compliance is the development of an understanding of the scope of the issue that must be addressed. Where is personal data maintained in your organization? Who is responsible for the collection, custody and use (*i.e.*, processing) of that data? Who has access to it?

In addition to the human resources department, the information technology department no doubt has access to and processes personal data, as do the finance, accounting and benefits administration groups. The legal department also should not be overlooked as it may have contracts, medical information, and even may have exchanged employee rosters while in merger discussions or when performing a due diligence inquiry. Finally, do not forget about marketing, even as a potential repository of employee data, in the form of resumes and other materials used to market the capabilities of certain of your employees.

A single person (typically, a chief privacy officer) should be ultimately responsible for ensuring that these departments are communicating with each other about their information-handling practices to avoid the "silo effect" on data flow management. This phenomenon occurs when each department follows its own myopic practices and procedures, without considering the organization's overall needs, making it extremely difficult to obtain an accurate picture of information handling within the organization. The privacy officer can conduct *ongoing* data audits to mitigate or eliminate the "silo effect."

Effective data audits require specialized expertise—particularly in information technology. The best audits are performed with the assistance of an outside privacy consultant or firm that has experience in developing detailed, "living" data flows. If you feel that your company has the internal expertise to conduct such an audit, be sure to make expectations clear in terms of the need to consult with multiple departments and to compare policies/perceptions with actual data-handling practices.

#### 3. Mount An Aggressive Internal Sales Campaign.

Like so many other compliance issues that in-house lawyers and human resources professionals confront, compliance with the Safe Harbor Principles hardly sells itself. Instead, it might be viewed as just another costly and potentially time-consuming exercise, pushed by the lawyers, that produces no economic return.[15]

---

[14] It is important that your company implement a compliance plan in consultation with in-house or outside counsel. The steps discussed below are intended as a general "how to" list, rather than a specific prescription for any particular corporation.

[15] Compliance could well be both costly and time consuming. However, the argument that compliance produces no return is no truer for data protection than it is for any other compliance issue. If a company wants to raise capital by publicly selling equity in the business, it must comply with the securities laws as the price of doing so. The same can be said for data protection compliance.

Selling compliance should focus on the draconian consequences of protracted non-compliance—particularly the "information death sentence" that could cut off all EU-generated data and require erasure of all data which your company unlawfully imported from the EU. In addition, the risk of substantial corporate fines under the laws of many of the Member States for non-compliance is of real consequence. And, of course, the spectre of personal liability, including both criminal and civil exposure, for senior executives generally gets attention.

Keep in mind that you can emphasize the benefits of compliance (*e.g.*, earning employee and customer trust) in addition to warning of the risks of non-compliance. Privacy should be sold internally as central to the organization's values and as a vehicle for building competitive business advantage.

**4. Audit And Modify Contractual Relationships With Personal Data Transferees.**

Most companies transfer at least some personal data to third parties for processing. This would include, *inter alia*, the transfer of data to a payroll service that prepares paychecks and tax reporting information and the transmittal of other data to a health insurance provider. Before transferring any data, it is important that your company determine whether these third parties have adopted the Safe Harbor Principles or have otherwise been found compliant with the EU Directive or the national law of an EU Member State. If not, then your company will be required to negotiate an agreement with the third-party processor to adhere to privacy principles at least as stringent as the Safe Harbor Principles. This process will provide a measure of protection to your company should the third party mishandle personal data that your company transferred to it.

In general, unless the third party has certified its compliance with the Safe Harbor Principles (which can be determined through the Department of Commerce's Web site), you must secure the third party's agreement to limit its processing of data to those purposes stated in the contract, for which you should have obtained employee consent.

**5. Implement A Data Protection Policy And Provide Training.**

The written data protection policy is a primary component of compliance with the Safe Harbor Principles. The policy should affirm your company's commitment to protecting employee personal information and should describe how the commitment is, or will be, delivered. It is mandatory that the policy address specifically each of the seven Safe Harbor Principles. (Those principles are discussed in detail at page 7, above.) The policy must describe present and anticipated personal data handling procedures. The company also should harmonize the privacy policy applicable in the United States with the policies developed for its operations in the EU.

Adherence to the Safe Harbor Principles requires more than the distribution of a policy statement which will only collect dust on employees' "to-read" pile, or worse. Given the radically new conception of privacy, at least for the United States, engendered in the Safe Harbor Principles, employee training will be critical to your company's successful compliance efforts. Indeed, a commitment to employee training is a mandatory part of the Safe Harbor certification process.

Training should be conducted across all levels of the organization, from the most senior management to front-line employees. Basic training for *all* employees should establish a privacy "baseline." Key information handlers and policy makers with the authority to establish data-processing policies should receive more intensive, advanced training.

**6. Notify And Obtain Consent To Disclosure From New Hires And Existing Employees.**

Three of the seven data protection principles can be satisfied by compliance with the notice and consent requirements. Specifically, by crafting and publishing appropriate notification of the use(s) to which your company will apply personal data and by receiving prior consents from new and existing employees, your company can achieve compliance with the notice, choice and onward data transfer principles.

Much like other notices typically provided in employment applications, such as notification of at-will employment and penalties for falsification of the application, the notice to job applicants can be included in the employment application. The notice should explain in plain language the intended uses of personal data. Other logical locations for written notice would be the company's form offer letter in the United States (and wherever else employed) and in employment contracts in jurisdictions where they are used. It must be remembered that if sensitive data is to be processed, employees must be given an explicit choice of whether or not to permit the processing, and not just be given a chance to "opt-out."

**7. File Requisite Papers With National Data Protection Authorities.**

Every European entity owned and/or operated by your company that processes personal data must register with the appropriate local data authority whether or not your company opts to join the Safe Harbor. The entity's failure to register with the local authority can have substantial repercussions.[16]

It must be remembered that before data are transferred to the United States for processing, the national laws of the Member State in which the entity is located regulate the data's processing, even if your company certifies adherence to the Safe Harbor Principles. The Safe Harbor Principles control only the processing of data in the U.S.

**8. Develop A Means For Keeping The Transferred Personal Data Current And Accurate.**

The Safe Harbor Principles require data processors to implement reasonable procedures intended to make sure that personal data is complete, up-to-date, and accurate. Reminders to employees to notify the company of all changes in status, address, and telephone number as they occur are one measure that can be implemented easily. Better yet, each employee can be required to confirm periodically the accuracy of the personal data the company maintains about him/her, thereby ensuring that your company will not be sued on behalf of the forgetful employee for maintaining outdated data. This requirement also should provide further impetus to adhere to the company's record retention procedures and to destroy dated material in accordance with the company's data destruction policy.[17] The company should maintain a record of each employee's additions and corrections and notify third parties to whom the company has sent erroneous data of these changes.

**9. Review And Enhance Security Measures In Place To Keep Personal Data Safe From Theft, Loss, Or Destruction And Misuse.**

Presumably your company has some security measures in place that, at a minimum, enable it to enforce its confidential business information and trade secret policy and to protect its electronically stored data from hackers. These measures should give your company a running start towards complying with the security requirements of the Safe Harbor. Indeed, many of the measures that should be implemented to comply with this Safe Harbor Principle are closely similar to those that we suggest to companies to protect their confidential business information. The goal is similar: to prevent theft, unauthorized use, and tampering with corporate data.

The following points and precautions are among those recommended:

- At the audit phase (step 1, above), identify every location where personal data from EU sources are kept, handled and otherwise processed;
- If you have a training program for handling trade secret and/or other confidential business information, add personal data from EU entities (at a minimum) to the types of data and documents which should be maintained and used in a manner calculated to preserve their confidentiality; train employees in each department identified in your audit (above);
- Implement and deploy prudent security controls, procedures, and devices to ensure that access to personal data is limited to those having a legitimate

[16] In the U.K., for example, a data processor is strictly liable for failing to register and is subject to significant fines.

[17] Care must be exercised not to be overzealous in purging inaccurate or dated information inasmuch as administrative agency regulations at both federal and state levels require retention of personnel file material, for example, for several years after the employment relationship ends. Record retention policies generally factor these requirements into the retention periods that they prescribe.

business reason for access; this should include measures such as requiring password protection for personal data maintained in your network, forbidding fax transmission of personal data except to and from a continuously monitored designated secure fax machine, use of firewalls, monitoring access to personal data on your network, and care in disposal of printouts, superseded data, and back-up data that is replaced;

- Enforce your security policies and procedures by imposing discipline for security breaches, carelessness, and other acts of non-compliance.

**10. Develop Procedures To Allow Employees Reasonable Access To Their Personal Data.**

Reasonable access and the opportunity to correct are a fundamental right of data subjects under the EU Directive and the Safe Harbor Principles. Those companies having operations in states such as California that recognize a similar right of reasonable access should already have a procedure and/or a policy in place that can be applied to data transferred from the EU. The policy and procedures developed should stress the need for reasonableness in the timing, frequency, and scope of the personal data request, and may impose a requirement for specificity in identifying the data for which access is sought.

## D. IMPLEMENTING OPTION THREE: CONTRACTUAL DATA-PROTECTION SAFEGUARDS

"Data-transfer contracts" most likely would be a useful compliance option for businesses which receive routine transfers of discrete categories of personal data from independent affiliates or separately incorporated subsidiaries located in the E.U. One example would be a U.S.-based franchiser which receives from its franchisees, for marketing purposes, specific categories of information about each customer. Another example would be a U.S.-based corporation that maintains a database of basic identification information for all employees, including those working for a single small subsidiary headquartered in Brussels.

If your business is like those described above, then you most likely could do without the data-processing overhaul necessary to comply with the Safe Harbor Principles. Instead, you could rely upon "data-transfer contracts" by following the implementation steps described below.

**1. Determine Whether The Structure Of Your Company Permits Taking Advantage Of This Option.**

A data-transfer contract necessarily requires the existence of two legally distinct entities to participate as parties. If your company's operations in Europe are not organized as a separate legal entity, then your company will not be able to utilize this option.

**2. Identify The Necessary Exports Of Personal Data.**

Because each data-transfer contract must be specific to a particular data export, or category of data exports, your company will need to identify each data export, or category of data export, for which your company requires approval from the relevant data protection authority. Your company should be able to use the results of the assessment described in paragraph A.2, above, for this purpose.

**3. Complete A Data-Transfer Contract And File The Contract With The Relevant Data Protection Authority.**

The model data transfer contract approved by the EU Commission is available at http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/1539en.pdf. Most of the required contract language has been predetermined. However, the contracting parties will have to provide the following information: (a) an identification of each party to the contract, (b) an identification of the data subjects, or categories to whom the exported data relates, (c) a description of the categories of personal data to be exported, (d) the purpose of the data export, (e) the persons to whom the exported data may be disclosed, (f) the length of time that the data importer will store the exported data, and (g) the Member State whose law will govern the contract (which will be the state in which the data exporter is located). To obtain the principal benefit of these contracts, automatic approval of the data export, the executed contract should be filed with the data protection authority in which the data exporter is located.

**4. Establish And Implement Policies And Procedures To Ensure Compliance With The Data-Transfer Contract.**

Clause 5 of the model contract describes the obligations of the data importer with respect to the imported personal data and the subjects of that data. Most of these contractual requirements are similar to the requirements of the Safe Harbor Principles. Significantly, data exported under a data-transfer contract may be used, and further disclosed, only for the specific purpose identified in the contract. In contrast, under the Safe Harbor Principles, the data importer may use or disclose the imported personal data for any purpose which is *compatible* with the purpose disclosed when the initial collection of the personal data occurred. Bear in mind that your company must find some way to effectively segregate and track the imported personal data. There is an obligation to ensure that the data are not "mixed" with personal data not subject to the contract and then processed in breach of the contract.

**5. Ensure That Any Third Party To Whom Your Company Might Transfer The Imported Personal Data Agrees To Provide Adequate Privacy Safeguards.**

The model data-transfer contract also imposes upon the data importer the duty to ensure that any third party who receives the imported data will provide equivalent privacy safeguards. Consequently, the person ultimately responsible for contract compliance must develop a list of agents and subcontractors who might be called upon to process the imported personal data.

Each agent and sub-contractor should be required to agree in writing to provide the same privacy safeguards as the data importer is required to provide. The data importer also should seek to obtain from each agent and sub-contractor an agreement to indemnify the data importer from any penalties or damage awards resulting from the third-party's privacy violations. The agent or sub-contractor also should be required to obtain insurance coverage, if available, for such violations.

**6. Be Prepared To Litigate Compliance Disputes In The EU State Of The Data Exporter.**

The model data transfer contract opens the door to litigation in a jurisdiction foreign to your company—the data importer. The model contract specifically provides that (a) the data subject is a third-party beneficiary of the contract, (b) the data subject has the right to choose the forum in which any dispute over contract compliance will be resolved, (c) the parties consent to jurisdiction in the EU Member State in which the data exporter is located, and (d) the law of that state will govern resolution of any dispute between the data subject and the contracting parties.

Given these contractual rights, the data subject almost surely will choose to exercise them so that he or she can litigate close to home. Because locating competent, qualified, and compatible counsel in a foreign country could be time consuming, your company should work to locate counsel of choice well in advance of any dispute.

## Conclusion

The time to address the EU's new data protection regime has arrived. To date, European data protection authorities may not have actively enforced the limitations on personal data transfers to the U.S. National data protection authorities, initially focused on implementation of national data protection laws. There is, however, every reason to believe that this implementation phase is coming to an end as employees in the Member States become more familiar with their rights under the EU Directive and the national laws of the Member States and employers become more familiar with their obligations. Recent reports that E.U. data protection authorities are dissatisfied with the slow pace of compliance with national implementing laws by U.S.-based businesses suggests that those authorities may be looking for a test case as a clarion call to compliance.

You, of course, do not want your business to be that broadly publicized test case, but you will not be able to avoiding that ignominious end with hasty decision making. Selecting the proper strategy in this emerging area at the intersection of privacy law and employment law will require careful study and a commitment of resources. But, making the right choice now should help your company avoid substantial administrative penalties, civil liability, criminal sanctions for it and some of its executives and a potentially catastrophic disruption of data flows, while contemporaneously resulting in a significant competitive advantage.

## Authors

**Shanti Atkins, Esq.**
*Littler Mendelson San Francisco*
650 California Street, 20th Floor
San Francisco, CA 94108.2693
Phone: 415.677.3140
satkins@littler.com

**Philip L. Gordon, Esq.**
*Littler Mendelson Denver*
One Tabor Center
1200 17th Street, Suite 2850
Denver, CO 80202.5835
Phone: 303.575.5858
pgordon@littler.com

**Scott J. Wenner, Esq.**
*Littler Mendelson New York*
885 Third Avenue, 16th Floor
New York, NY 10022.4834
Phone: 212.583.2664
swenner@littler.com

**Gary E. Clayton**
*Founder, Chairman Privacy Council*
1300 Arapaho Road, Suite 300
Richardson, TX 75081
Phone: 972.997.4044
gclayton@privacycouncil.com