Legislation & Guidance

E.U. Data Protection Requirements: An Overview for Employers

By Miriam Wugmeister, a Partner in the New York office of Morrison & Foerster, and Karin Retzer, an Associate at Morrison & Foerster in Brussels. Miriam Wugmeister may be contacted on tel. (+ 1) *202 506* 7213 *or at mwugmeister@mofo.com. Karin Retzer may be contacted on tel.* (32) *23470400 or at kretzer@mofo.com.*

Summary

Many foreign companies operating in the European Union are unaware that their traditional business practices may violate European Union [1] and Member State laws regarding personal data protection. The European Union Data Protection Directive 95/46/EC (the "Directive") regulates the collection, use, and transfer of individually identifiable personal information about employees, such as name, address, telephone number, and marital status, as well as information such as salary, bonuses, terms of an employment contract, and performance appraisals. In addition, the transfer of employee information to another entity, even a related corporate affiliate, without providing explicit notice to employees and in some cases obtaining consent from employees may be considered a violation of Member State laws. Thus, for example, if a company with operations in the United Kingdom provides information regarding individual employees to the home office in the United States that company must comply with the U.K. Data Protection law. The potential liability for employers failing to abide by these laws can be quite high.

The Spanish Data Protective Authority, for example, recently fined an organisation nearly 840,000 euros (approximately US$900,000) for sharing customer data with a subsidiary organisation and fined another organization 1.08 million euros (approximately US$1.17 million) for disclosing protected personal information to the public. Companies with operations in the European Union, especially those that centralise human resources information in databases located outside the European Union or regularly transfer employee data among offices outside the European Union, may have to change the way they collect and use employee data.

Virtually every company with employees in a Member State in the European Union must comply with the Directive and Member State laws implementing the Directive. These laws apply to the collection, processing, and transferring of employee personal data, online and offline and manual, as well as automatic. Employers must have appropriate legal grounds to collect and process personal employee information and transfer that data to another entity, even an affiliated organization such as a parent company or a subsidiary.

In addition to specific regulations regarding the collection and use of personal data within the European Union, the Directive also requires Member States to restrict the transfer of personal data to only those countries outside the European Union that provide "adequate" data protection. "Adequate" is not defined by the Directive or by any of the Member States. The Directive also provides several exceptions that allow for international transfers of personal information where there is no adequacy determination in place for the relevant jurisdiction.[2] The rules are extensive and still evolving. They also differ significantly from Member State to Member State. Given the possible fines and potential injury to reputation and goodwill that may result if a serious privacy violation is publicised, it is imperative that employers review and adopt appropriate policies and practices.

Recommendations for Employers

Limit Information to Essential Information

Any company operating in the European Union has to comply with all relevant Member State data protection laws. A company should, therefore, know what employee information it collects, how such information is used, to whom it is disclosed and to what countries it is transferred. Such information and uses should be catalogued by the company. Special attention should be paid to any information collected that is considered sensitive information, because it requires special handling. Once a company understands what data it collects from its employees, the company should examine the purpose(s) for collecting the information to ensure that it has specified, explicit, and legitimate bases for such collection so that the Member State requirements are met. Thus, all information must be tested under these standards and any "nice to have" but unessential information should not be collected.

Review Internal Procedures

A company must put procedures in place to ensure the accuracy of information and purging of information no longer required for the purposes for which it was collected. Further, the company should evaluate its technical and organisational measures for ensuring that employee information is protected against unauthorized disclosure or access and also ensure that appropriate training is in place for staff that have access to personal data of other employees. The company should ensure that it is in compliance with registration requirements in those Member States in which the company has employees and that require registration.

Review Legal Basis for Transfer of Information

As part of its employee data collection and use inventory, a company should review whether it transfers any employee data to the United States, or other third countries that have not been declared "adequate" by the European Union Commission. If a company does, indeed, transfer data to the United States, the company should have a legal basis for the transfer of such information, *e.g.*, ad hoc contracts, model contracts, consent, and bring itself into compliance with the requirements of the chosen basis.

Monitor Legislative Changes

Finally, given the intense discussion on collection and use of employee information currently underway at the European Union Commission and many of the Member States, companies should routinely monitor new developments and adjust their procedures accordingly.

Introduction

Businesses that collect and use employee personal data in the European Union face an extensive legal framework, which unlike the privacy laws and self-regulatory regimes adopted in the United States, also imposes strict privacy conditions on employee data. The E.U. Data Protection Directive 95/46/EC[3] applies to both employee and consumer personal information, and the Member States' laws enacted to implement the Directive also apply to employee and consumer personal information. These laws impose substantial requirements on the collection and use of virtually all employee data while those data are in the European Union.

In addition, these laws restrict the transfer of that information from the European Union to third countries, such as the United States, unless the third country has been found to provide an adequate level of protection or the employer can identify another legal basis for the transfer. Accordingly, any employer operating in the European Union must first conform its data practices to the Directive and Member State laws while the data are in the European Union. And, when transferring employee data from the European Union to third countries, employers also must identify and implement a legal basis for such transfers. Employers operating in the European Union that collect or process personal information in the European Union without adhering to Member State laws or transfer personal information from the European Union to a country without "adequate" protection or a relevant exception may incur substantial legal liability.

The Directive is framework legislation and requires each Member State to enact implementing legislation. All but one Member State (France) have now done so. The Directive sets a floor for the Member State legislation, and in some instances it may also set a ceiling. It does not, however, prohibit divergences among Member State laws. Accordingly, employers doing business in the European Union must inform themselves about and comply with all the terms of the specific Member State data protection laws that are in effect in the countries in which the companies have employees.

This article is intended as a guide for companies with employees in the European Union who are evaluating their employee data practices. It provides an introduction for employers to

- the Directive;
- how human resources data are defined in the European Union;
- basic European Union data protection requirements;
- the legal grounds for transferring employee information to countries outside the European Union; and
- practical steps for companies operating in or receiving employee data from the European Union should take to ensure compliance with European Union legal requirements.

Overview of the Directive and Its Application to Employee Data

Consistent with European legal tradition, the Directive sets forth a broad, highly regulatory, and inclusive approach to privacy issues. The primary objectives of the Directive are:

- to protect individuals with respect to the "processing" of personal information (personal information is defined as information relating to an identified or identifiable natural person); and
- to ensure the free movement of personal information within the European Union through the harmonization of national laws [Article 1].

The Directive is extraordinarily broad in scope. It applies to all processing of data, online and offline, manual as well as automatic, and all organisations holding personal data. Only data used "in the course of purely personal or household activity" are excluded from its reach [Article 3]. Thus, an employer's collection and use of employee data clearly falls within the ambit of the Directive. The Directive establishes strict requirements for the processing of personal information. "Processing" of data includes any operations involving personal information, except perhaps its mere transmission. For example, copying information or putting it in a file is viewed as "processing." An employer should keep in mind that "sensitive" data, such as that pertaining to racial or ethnic origins, trade union membership, political or religious beliefs, or health or sex life, may not be processed unless such processing comes within limited exceptions [Article 8].

The Directive also requires each Member State to establish an independent data protection authority (DPA) to supervise the protection of personal data [Article 28]. An employer that is processing data must register with (or notify) the DPA prior to processing any data [Article 18], unless the employer fits within an exemption provided under a Member State law [Articles 18 and 19]. This requirement mandates that prior to carrying out any processing, an employer must provide the relevant DPAs with information on the purpose of the processing, the categories of individuals whose data are being processed and the types of data relating to them, the categories of the recipients to whom the data may be disclosed, proposed transfers to third countries, and the security measures in place.

What are "Human Resources Data?"

Despite its applicability to employee data, the Directive does not provide any specific guidance on the processing of data in the employment context, nor does it specifically define human resources data. The definition of "personal data" is extremely broad, however, and, as noted above, encompasses

> *"any information relating to an identified or identifiable natural person . . .* An identifiable person is one 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." (Emphasis added.) [Article 2(a)].

An employer will also find, for the most part, little guidance in Member State laws, which either fail to define human resources data or do so very generally. A definition of human resources data often must be inferred from data protection registration forms that require an employer to provide the purpose of the employee database and its specific use. The inferences that may be drawn from the examples of human resources data on these forms are very broad and suggest that all personal information about employees collected by employers is covered.[4] Accordingly, an employer doing business in the European Union should assume that *any* information relating to prospective, present, or past employees collected in *any* form will be subject to the

protections of the Directive and must be handled in a manner compliant with Member State data protection law.

E.U. Data Protection Requirements Applicable to Human Resources Data

While all the Directive's data protection principles apply to personal data in all contexts, in some instances the principles may apply differently in the employment context than in other contexts.

Legitimacy: Establishing the Legal Grounds for Processing Employee Data

An employer must have appropriate legal grounds to process personal information [Article 7]. An employer must meet this legitimacy standard for processing employee data, and such processing must be "necessary for the achievement of the objective in question rather than merely incidental to its achievement" ("Working Party Opinion").[5] An employer may establish this legitimacy by several means, with the most relevant to the employment context including:

- processing necessary for performance of the contract between the company and the employee;
- processing necessary for compliance with a legal obligation;
- processing necessary for purposes of a legitimate interest by the controller; and
- processing with employee consent.

Performance of Employment Contract

An employer may process most employee information based on the grounds that the processing is necessary for the performance of a contract to which the employee is party [Article 7(b)], *e.g.,* the "employment contract". The DPAs generally take a fairly strict view of what information is "necessary" for performance of the contract and make their determinations on a case-by-case basis. Data such as name, home address, date of birth, appraisals and promotions, job title, department, terms and conditions of employment, supervisors, salary, promotions, and reviews have been found to be necessary to the performance of an employment contract. (In some Member States, what is necessary for performance of the employment contract may be interpreted more strictly than in others, In those states, companies should consider establishing additional legal grounds for processing employee data, such as employee consent.

Compliance with Legal Obligations

An employer may also establish legitimacy if the data processing is "necessary for compliance with a legal obligation." [Article 7(c)]. For example, an employer may have a legal obligation to provide to government authorities information on tax and social security status and the number of days absent due to sickness. To the extent that such information is *sensitive* information under Article 8 of the Directive, such as data on specific illnesses, under many Member State laws it is also necessary to obtain consent from the individual, despite the existence of the legal obligation.

Legitimate Interests of the Controller

An employer may process data if it is

> "necessary to meet the legitimate interests pursued by the controller or by a third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject . . . ." [Article 7(f)].

For example, collection of certain information for employee performance assessment purposes may be considered a legitimate interest of the controller. Employers may not, however, use the data in a manner that would "unjustifiably prejudice the rights and freedoms of the data subject," and care should be taken in utilising this ground for processing.

Employee Consent

At first glance, employee consent appears likely to be an employer's simplest option for legitimising its data processing practices as it could be drafted to cover all uses of the data without question. In most Member States, the consent would be opt-out consent, unless the personal information in question is sensitive, in which case a more onerous opt-in or affirmative consent is required. This method, however, poses significant issues for the employer. Whether "consent" may be freely given in the context of an employment relationship has been the subject of much debate among the Member States. Several Member States maintain the view that an existing employee cannot freely give consent. Moreover, the Working Party Opinion takes the view that:

> where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data, it is misleading if the employer seeks to legitimize this processing through consent Reliance on consent should therefore be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment.

Accordingly, in the Member States that take this position, an employer who relies on consent to legitimize data processing in the employee context may face significant risks and should consider another ground for processing. In addition, this method may provide at best only a short-lived solution for an employer because employees may withdraw their consent at any time.

Collection and Use of Employee Data

Proportionality

In addition to establishing grounds for legitimate data processing, the employee information an employer collects "must be adequate, relevant and not excessive" in relation to the purposes for which the data are collected and/or further processed [Article 6.1(c)]. Thus, an employer must gather information and use it in the "least intrusive way." The concept of proportionality is closely related to legitimacy.

Finality of Processing.

Under the Directive, the employee data an employer collects must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes [Article 6]. Thus, an employer may not use employee information collected for a legitimate purpose for any other "incompatible" purposes without the specific consent of the employee. For example, home addresses collected for payroll purposes should not be used for direct mailings without specific consent. An employer, however, would not be prohibited from using the data for a "compatible" purpose, such as calculating travel allowances.

Notice

The Directive further requires the employer (a data controller) to disclose its identity, the purposes of the

processing, categories of recipients of the data, and the right of access and correction [Articles 10 and 11]. Thus, even if an employer's processing is legitimised on the grounds that it is necessary to complete the contract and consent is not necessary, the employer may still have to provide notice to employees about what employee data the employer is collecting, both directly and from other sources, and how the information will be used. Therefore, companies should provide employees with appropriate disclosures about the collection and processing of their personal data.

Accuracy and Retention

Under the Directive, personal data must be accurate and up-to-date [Article 6.1(d)]. To comply with this requirement, an employer must take reasonable steps to ensure that employee data maintained by the employer meet these requirements. Moreover, the employer should not maintain data in a form that identifies specific individuals any longer than necessary for the purposes for which the information was collected or processed.

Security

Under the Directive, an employer must institute technical and organisational measures to ensure that personal data is maintained securely and protected against unauthorised disclosure or access. Thus, an employer wishing to comply with the Directive will need to establish security procedures and access controls for employee data. Some countries have enacted regulations that set forth in great-exacting detail the particular technical and organizational security measures that must be implemented.

Employee Access

The Directive requires that an employer provide each employee the right to access and correct information maintained about him or her [Article 12]. The Working Party Opinion shed light on this requirement by stating that employers must provide employees with access "without constraint at reasonable intervals and without excessive delay or expense." Access includes confirmation about whether data relating to the employee are being processed, the purposes of the processing, the categories of data concerned, and the recipient or categories of recipients to whom the data are disclosed. In addition, the Directive also requires that an employer permit an employee to correct, erase, or block data that do not comply with data protection law, for example, if the data is incomplete or inaccurate. The Article 29 Working Party Recommendation 1/2001 on Employee Evaluation Data,[6] which provides that personal data includes "subjective judgments and evaluations," also recommends that employees be provided with notice about and afforded a right of access to such data.

Other Requirement

In most Member States, an employer must inform the DPAs before the company may transfer information outside the European Union to countries that do not provide "adequate" privacy protection, register the company's database, and obtain the DPAs' approval. In addition, the Directive sets forth many other requirements that an employer should consider, including prescribing specific rules where personal information has not been obtained from the individual and where automated individual decision-making and direct marketing are involved.

Employer Liability under E.U. Law

For the most part, enforcement of Member State privacy laws is complaint driven. Employees who believe the law has been violated may bring a complaint either to the relevant DPA authority or to a court. Given the expense of bringing suit, the lack of contingency fees in E.U. countries, and obligations in the European Union for the losing party to pay both parties' fees, many individuals choose to bring their complaints to their DPAs.

An employer may be liable to an individual for compensatory damages as a result of unlawful data processing [Article 23]. Employers' possible liability differs significantly from Member State to Member State. For example, German law allows for a variety of penalties and remedies, including injunctions and orders to comply. The German law also provides for fines up to 255,000 euros (approximately US$275,000), and criminal penalties in extreme cases. In France, fines may be assessed up to a maximum of 45,000 euros (approximately US$48,500) and criminal penalties imposed of imprisonment of not more than three years. The U.K. law provides for a variety of sanctions similar to those described for the German law, including criminal penalties. The maximum fines in Spain are considerably higher and can be as much as US$500,000. In assessing their risks under European Union privacy laws, employers also should consider injury to reputation and goodwill that may result if a serious privacy violation is publicized.

Transfers of Employee Information to Third Countries

In addition to covering the collection, use, processing, or disclosure of personal data within the European Union, the Directive also requires Member States to restrict the transfer of personal data, including human resources data, to countries that provide "adequate" data protection. Neither the Directive nor Member State laws define "adequacy," thus leaving a great deal of uncertainty about whether a particular privacy framework would be deemed "adequate" by the European Union and information may continue to be transferred.

Article 26 of the Directive provides several exceptions that allow for international transfers of personal information where there is no "adequacy" determination in place for the relevant jurisdiction. These exceptions are similar to those that are provided by the Directive for legitimizing data processing in general and include situations where:

- the data subject has given his or her unambiguous consent;
- the transfer is necessary for the performance of the contract with the individual; or
- the controller has entered into an appropriate contract, which if individually negotiated, may require approval of the Member State DPA ("ad hoc contracts"), or which incorporates certain standard contractual clauses that have been approved by the European Union Commission ("model contracts"; or
- the controller and the corporate affiliate receiving the data maintain and police binding corporate rules or codes of conduct, which also require approval of some Member State DPAs.

Relying on these exceptions in the cross border contract has significant drawbacks, however. These drawbacks are discussed below.

After the enactment of the Directive, concerns arose over whether the European Union would grant the United States an adequacy determination, given the disparity between the European Union and the United States approaches to privacy. Accordingly, in 1998, the United States Government

and the European Union Commission began negotiations to develop an alternative basis for data transfers to the United States. These resulted in the safe harbor privacy accord ("safe harbor"). The safe harbor provides another basis for transferring personal data to the United States in addition to the exceptions set forth in the Directive.

Employee Consent for the Transfer of Data

Employee consent for the transfer of personal data outside the European Union is distinct from, for example, the consent required to disclose such data to third parties within the European Union Although the Directive requires "unambiguous" consent in both instances [Articles 79a) and 26.1(a)., if consent is relied on to legitimise disclosures to third parties within the European Union, in some Member States an employer need only obtain opt-out consent (unless sensitive information is involved). Where consent is required to legitimize cross border data transfers from the European Union to third countries, nearly all the Member States interpret unambiguous consent to require opt-in or affirmative consent. Many Member States also require the employer to inform the employee that the data will be transferred to a country that may not ensure "adequate: privacy.

As previously discussed, the view taken by some Member States that consent from existing employees is either suspect or invalid means that in those countries it is also a risky proposition for employers to rely on even opt-in employee consent for cross border transfers. At a minimum, employers that rely on employee consent will need to examine whether the Member State from which the data are to be exported accepts employee consent as a valid basis for legitimising such transfers. The Working Party Opinion casts further doubt on the use of employee consent to legitimise transfers of employee data out of the European Union Given the uncertainty of whether employee consent may be relied upon in certain Member States and proposed legislation in others, employers wishing to transfer employee data to the United States (or other countries that do not meet the European Union "adequacy" standards) may wish to consider relying on grounds other than employee consent for such transfers.

Information Necessary to Complete the Employment Contract

Employers who transfer employee information on the basis that it is necessary to complete the employment contract are limited in the purposes for which they may use the information once it is transferred out of the European Union Thus far, there has been no detailed discussion in the European Union of what would be considered "necessary" in this context. As noted above, many Member States take a fairly narrow view of what is necessary to complete the contract. When relying on this ground for transferring employee information from the European Union, employers should be cautious about using such information after it has been transferred to do more than pay employees and provide benefits. Using employee information for purposes such as creating an employee telephone list or tracking employee mobility and travel availability may not be permitted if a company relied on this exception in transferring the data.

The need to transfer for the purposes of performing a contract also extends to those cases where an agreement is concluded between a European Union data controller and a non-European Union third party involving a transfer to the third party if such transfer is carried out in the interest of the data subject. For example, a United States company with offices in the European Union could use this as legal grounds to transfer data concerning its European Union employees from the European Union to a third-party company in the United States to enable such company to provide a health or pension scheme to its European Union employees.

Contracts

Ad Hoc Contracts

Ad hoc contracts are individually negotiated contracts and are concluded between the data exporter in the European Union and the data importer located outside the European Union. In most Member States , these contracts must be approved by the relevant Member State DPA. In the employment context, the contract would be between the employer in the European Union and its United States affiliate. Ad hoc contracts vary from country to country, but generally provide that the data must be processed consistently with the Directive and, in many instances, with the laws of the Member State from which the data are exported.

A major advantage of ad hoc contracts is that they have served as a legal basis for transferring personal data from Europe for over ten years and, therefore, provide a great deal of legal certainty for companies relying on them. Ad hoc contracts, however, have several significant disadvantages as well. While the purpose of the Directive is to harmonise data protection law throughout the European Union, differences still remain among the Member States' data protection laws. Consequently, when an employer relies on ad hoc contracts to legitimise the transfer of data from the European Union, the employer or company would need to continue to track data received from the Member States by country of origin to' ensure that the data are handled in compliance with the appropriate Member State data protection requirements. In addition, employers considering this option need to consider scheduling requirements because extensive delays may occur due to the approvals of ad hoc contracts that are required in many Member States. Approvals generally take a minimum of one to two months to obtain and may take longer if the DPA has questions about the transfer or the requisite forms were not completed properly in the first instance. Subsequent additional approvals also may be required, for example, if changes are made in the processing of or type of personal information collected.

Model Contracts

The Commission formally adopted model contract clauses for transfers *of* data from one controller to another controller located outside the European Union[7] in June 2001, and the clauses went into effect in September 2001. Many had hoped that model contracts, which are intended to provide one form contract useable in all E.U. countries and require no approval by individual DPAs, would create a workable and substantially more streamlined data transfer process. Unfortunately, it appears that the model contracts' drawbacks may outweigh its advantages.

The model contract clauses approved by the European Union allow the data importer three different options. It may elect to comply with the national law of the data exporter, with the Mandatory Principles attached to the model contract,[8] or with a Commission adequacy decision, provided the company is located in the jurisdiction to which the decision applies and the company also complies with yet other mandatory privacy principles also attached to the model clauses.[9] These options leave companies with a burdensome and potentially unworkable scenario. For example,

if companies choose to comply with the national law of the data exporter and they have employees in several E.U. countries, as discussed above, companies may have to comply with multiple legal requirements of different Member States.

If companies elect to abide by the Mandatory Principles, these companies will be required to adhere to a higher standard than is required by the Directive. For example, under the Directive, information may be processed for the use for which it was acquired, as well as for any other compatible uses. The Mandatory Principles, however, more narrowly restrict uses of the information, allowing it to be used only for the specific purpose for which it was collected. Additionally, if companies choose to rely on the terms of a Commission adequacy determination, such as the safe harbor (discussed below), they have to "top up" and comply with stricter requirements than those set forth in the "adequacy" determinations. In both instances, companies will be limited in their uses of personal information so that it may only be used for the specific purpose for which it was collected, requiring employers to go back to their employees if the companies want to use employee data for additional purposes than those contemplated when the companies collected the data. In both instances, the companies' use of data would be more limited once the data are transferred from the European Union than while the data are still in the European Union.

The model clauses further require that:

- the data subject be made a third party beneficiary of the agreement;
- the data exporter and data importer be jointly and severally liable for any damages;
- the data importer submit to audit by the data exporter or an inspection body selected by the data exporter (and where applicable, in agreement with the DPA);
- the data importer have security measures in place that are appropriate to the risk; (v) the data importer warrant that it "has no reason to believe" that the legislation applicable to the data importer prevents it from fulfilling its obligations under the contract;
- the governing law of the agreement is the law of the Member State where the data exporter is established; and
- the parties agree to the jurisdiction of the relevant Member State courts.

These onerous requirements potentially create a host of difficulties for companies that choose to rely on model contracts. For example, a U.S. company would have to agree to be subject to the jurisdiction of each Member State from which it transfers data. Thus, the model clauses do little, if anything, to provide a less burdensome approach to data transfers from the European Union to third countries than the other alternatives provided by Article 26 of the Directive.

Binding Corporate Rules

The Article 29 Working Party, an advisory committee set up under Article 29 of the Data Protection Directive and consisting of representatives from the DPAs of the EU. Member States, issued a Working Document on Binding Corporate Rules for International Data Transfer on June 3, 2003 (hereinafter "Working Paper"). Corporate Rules may serve as another adequacy mechanism for facilitating data transfers between corporate affiliates, and they would allow for one set of rules for the entire corporation. The Working Paper, however, establishes very restrictive standards for corporate rules, requiring compliance with the strictest E.U. national regimes, and going beyond the requirements established in the Standard Clauses approved by the European Commission. The other obstacle to using binding corporate rules is that there is no streamlined mechanism for approving company-wide codes. In other words, corporate rules or codes may currently only be used to legitimise data transfers if they comply with the national provisions of the country from which the data is to be transferred. Each DPA would also have the authority to require changes to the corporate code. Unfortunately, as is evident from the Working Paper, little progress towards harmonisation, or at least co-ordination between the DPAs has been made. However, for some employers operating in Germany, Austria, the Netherlands, and the United Kingdom, binding corporate rules may be an attractive alternative as these DPAs appear more open for discussion.

Safe Harbor

As noted above, in response to the difficulties faced in satisfying the alternative grounds for data transfers provided under the Directive, the U.S. and the European Union negotiated and adopted the safe harbor. Under the safe harbor, U.S. companies that voluntarily decide to adhere to the self-regulatory safe harbor framework will be deemed "adequate" and data flows from the European Union to such companies may continue.

The safe harbor provides several advantages not provided by the other legal grounds for transferring data from the European Union. First, because all 15 Member States are bound by the E.U. adequacy determination, an employer that chooses to adhere to the safe harbor generally is subject to one privacy regime for all European Union personal data that are transferred to the United States. Secondly, the safe harbor provides a more streamlined approach for data transfers from the European Union and makes those transfers less expensive and bureaucratic because the safe harbor eliminates the need for prior approvals or makes such transfers automatic. Finally, the safe harbor principles also more clearly reflect the United States approach to privacy and to some extent moderate requirements of the Directive. Given the many disadvantages of transferring data from the European Union under the provisions previously discussed, many companies are considering the safe harbor as the legal basis for transfers of personal data from the European Union to the United States

General Safe Harbor Requirements.

For a U.S. employer to be eligible for the safe harbor, it must be subject to the jurisdiction of a

> "government body which is empowered to investigate complaints and to obtain relief against unfair and deceptive practices. . . in case of noncompliance with the [safe harbor] Principles."[10]

At present, only the Federal Trade Commission ("FTC") (under section 5 of the Federal Trade Commission Act) and the Department of Transportation ("DOT") (under 49 US.C. section 41712, which covers air carriers)[11] would satisfy this requirement, as only they have been recognised by the European Commission.[12] Therefore, only employers subject to the jurisdiction of either of those two agencies are eligible to join the safe harbor. Financial services institutions that are subject to the jurisdiction of the banking regulatory agencies and telecommunications common carriers (which are subject to the jurisdiction of the Federal Communications

Commission) are not eligible for the safe harbor at this time.

An organisation must publicly declare in its privacy policy statement that it adheres to the safe harbor in order to participate. To be assured of safe harbor benefits, an employer also should self-certify to the United States Department of Commerce. The Department of Commerce maintains and makes public a list of all organisations that file self-certification letters.

To be compliant, employers must comply with the complete safe harbor framework.[13] The operative framework includes the safe harbor principles and accompanying 15 frequently asked questions ("FAQs"),[14] as well as the European Union Commission's decision finding the safe harbor adequate. The safe harbor applies to both consumer and employee information. Furthermore, FAQ 9 specifically addresses human resources issues.[15]

While the safe harbor bears similarity to the Directive in many respects, it also provides more flexibility than the Directive. Similar to the Directive, the safe harbor principles require an employer to provide employees with notice of the purposes for which information about them is being collected and the types of third parties to which the information is disclosed as well as of the means for limiting the use and disclosure of information. An employer must provide employees the opportunity to choose (opt-out) when their personal information may be used for an incompatible purpose or disclosed to a third party other than an agent of the employer. An employer would be required to obtain affirmative opt-in consent for use of sensitive information.

The access requirements are less restrictive and provide explicit and extensive exceptions. The safe harbor limits the right to access with a "reasonableness" standard that is not included in the Directive. The right of access may be limited if

> "the burden or expense of providing access would be disproportionate (unreasonable) to the risks to the individual's privacy in the case in question or where the rights of persons other than the individual would be violated."[16]

Thus, an employer would have some flexibility in providing employee access to information. Finally, there is no requirement for appointment of a data controller or registration of databases as there is in some Member States.

Consistent with the safe harbor's self regulatory approach, companies that adhere to the safe harbor are required to make available a dispute resolution mechanism for investigating and resolving individual complaints as well as procedures for verifying compliance. An employer also is required to remedy problems arising out of a failure to comply with the safe harbor, and sanctions must be severe enough to ensure compliance.

Generally, the dispute resolution, verification, and remedy requirements can be satisfied by an employer in different ways. For example, generally companies may choose to comply with a private sector privacy seal program that incorporates and satisfies the safe harbor principles. Or, companies may satisfy the dispute resolution and remedy requirements by committing to cooperate with DPAs located in the European Union.

Safe Harbor Requirements Specific to Human Resources Data

Although employment data falls within the general purview of the safe harbor, the safe harbor subjects employment data to additional requirements. For example, with respect to employment data, employers have no choice but to agree to cooperate with the DPAs for the complaint resolution mechanism. In addition, in some instances, national requirements may continue to "run with" the data even after they are transferred from the European Union to the United States[17]

FAQ 9 makes clear that primary responsibility for the data remains with the company in the European Union. Therefore, even if an alleged mishandling of personal information involving a breach of the safe harbor framework takes place in the United States and is the responsibility of the United States organisation, the employer in the European Union would remain primarily liable. Although somewhat unorthodox, this approach does reflect the reality of how many companies would choose to deal with data protection compliance even after E.U. employee data are transferred from the European Union to other countries. Many if not most companies would prefer that employees based in the European Union address their data protection concerns first to the E.U. company, which will be far more familiar with the employee(s) and local requirements. At the same time, in the view of many companies, the safe harbor leaves employers in a better position than they would be if they had to rely on a model contract, with its more restrictive requirements, or on ad hoc contracts, with their burdensome requirements.

Employer Evaluation of Employee Data Practices

Any company operating in the European Union has to comply with all relevant Member State data protection laws. A company should, therefore, know what information relating to its employees it collects and how such information is used. Such information and uses should be catalogued by the company. Special attention should be paid to any information collected that is considered sensitive information, because it requires special handling. Once a company understands what data it collects from its employees, the company should examine the purpose(s) for collecting the information to ensure that it has specified, explicit, and legitimate purpose(s) for such collection so that the Directive's stringent "necessary" standard is met. Also, an employer should take into account when examining its practices that the proportionality requirement bars collection and use of information that is excessive in relation to the purposes for which it is collected. Thus, all information must be tested under these standards and any "nice to have" but unessential information should not be collected.

A company must put adequate procedures in place to ensure the accuracy of information and purging of information no longer required for the purposes for which it was collected. To comply with the notice requirement, a company should assess its practices and create appropriate descriptions of what the company collects about its employees and how such information is used and disclosed, and provide these descriptions to employees. In certain instances, it may be necessary for an employer to obtain informed employee consent.

Further, the company should evaluate its technical and organisational measures for ensuring that employee information is protected against unauthorised disclosure or access and also ensure that appropriate training is in place for staff members who have access to personal data of other employees. An employer may want to consider employment contracts that include confidentiality clauses for staff members handling employee data.

Finally, the company should ensure that it is in compliance

with DPA registration requirements in those Member States in which the company has employees and that require registration.

Assessing the Legal Ground(s) for Transfer of Employee Data from the European Union

As part of its employee data collection and use inventory, a company should review whether it transfers any employee data to the United States or other third countries that have not been declared "adequate" by the European Commission.[18] If a company does, indeed, transfer data to the United States, the company should determine the most practical ground on which it will transfer such information, *e.g.,* ad hoc contracts, model contracts, or consent, and bring itself into compliance with the requirements of the chosen ground.

Ongoing Considerations

Finally, given the intense discussion on collection and use of employee information currently underway in the European Union and many Member States, companies should routinely monitor new developments and adjust their procedures accordingly. For example, responses to the recently issued Consultation Document are likely to play an important role in shaping an initiative at the Community level and, therefore, affect community employment data practices.

---

1 Any reference to the European Union should be understood as referring to the territory of the European Economic Area ("EEA"). The Member States are Belgium, France, Germany, Iceland, Italy, Liechtenstein, Luxembourg, the Netherlands, Norway, Denmark, Ireland, the United Kingdom, Greece, Spain, Portugal, Austria, Finland, and Sweden.

2 Four counties have been determined to provide adequate data protection: Switzerland, Canada, Hungary, and the United States through the voluntary self regulatory system called Safe Harbor.

3 Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 0031-0050. The Directive took effect in October 1998.

4 For example, the Spanish registration form contains categories for employee management, management of payrolls, employee training, social security, and recruiting. The Working Party Opinion (as defined in the text) also gives examples of employment records covered by the Directive, which includes: "[a]pp1ication forms and work references, travel, payroll and tax information, tax and social benefits information, sickness records and annual leave." See footnote 5 below.

5 Article 29 Data Protection Working Party Opinion 8/2001 on the processing of personal data in the employment context, September 13, 2001, available at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp8en.pdf.

6 See Article 29 Data Protection Working Party Recommendation 1/2001 on Employee Data (5009/01/EN final), Adopted 22.3.2001, available at http://europa.eu.int/comm/internal_market/dataprot/wpdocs/wp42en.pdf.

7 See Commission Decision 2001/497/EC of June 15, 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC O.J. (L181/19) of 4.7.2001 available at http://europa.eu.int/comm/internal_market/en/dataprot/news/1539.pdf. The Commission is also in the process of considering standard contractual clauses for the transfer of personal data to third countries from a data controller to a data processor. See Draft Commission Decision (version August 31, 2001) on standard contractual clauses for the transfer of personal data processors established in third countries under Article 26(4) of Directive 95/46, available at http://europa.eu/int/comm/internal_market/en/dataprot/wpdocs/wp47en.pdf.

8 See footnote 7, Commission Decision 2001/497/EC of 15 June 2001, at Appendix 2.

9 See footnote 7, at Appendix 3.

10 See Section 314 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Interpret and Obstruct Terrorism Act of 200 I ("USA PATRIOT Act"), Pub. L. No. 107-56(2001).

11 See Article 1(2)(b) of the Commission Decision of July 26, 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the United States Department of Commerce, available at http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/dec2000520ec.pdf.

12 The E.U. wanted to ensure that a government body (state or federal) would provide safe harbor enforcement in the event that self-regulatory mechanisms did not operate appropriately. To date, only the FTC and DOT have agreed to enforce the safe harbor principles. Unless the banking regulators agree to enforce the safe harbor principles, United States financial institutions regulated under the banking statutes will not be eligible to participate in the safe harbor.

13 The European Commission requests that the U.S. agencies provide a letter stating that they will enforce the safe harbor framework. As the Annex attached to the safe harbor principles indicates, only the FTC and DOT agencies have done so.

14 The principles, FAQs and other safe harbor documents can be located at www.export.gov/safeharbor.

15 The 15 FAQs provide further guidance that clarifies and supplements the safe harbor principles on issues such as access, publicly available information, and public record information as well as sector-specific guidance for information processing by medical pharmaceutical, travel, and accounting firms.

16 FAQ 9 explicitly states that the safe harbor applies to the transfer of human resources data.

17 Safe Harbor Privacy Principles, July 21, 2000, available at http://www.export/gov/safeharbor/SHPRINCIPLESFINAL.htm.

18 Adequacy determinations have been reached for Hungary, Switzerland, Canada and the United States through the voluntary self-regulatory system called the safe harbor.