EU Data Protection Directive and U.S. Safe Harbor Framework: An Employer Update

By Stephen H. LaCount, Esq.

Overview

The European Union Data Protection Directive 95/46/EC ("Directive") went effective in October of 1998 with the objectives (i) to protect individuals with respect to the processing of personal information; and (ii) to ensure the free movement of personal information within the EU through harmonization of national laws. The Directive regulates the collection, use, and transfer of individually identifiable personal information about *employees* and *consumers*, such as name, address, telephone number and marital status. It also covers information relating to salary, bonuses, terms of an employment contract, and performance appraisals. Special handling and restrictions are mandated for "sensitive" data, such as that pertaining to racial or ethnic origins, trade union membership, political or religious beliefs, or health or sex life. All methods of collection and processing are encompassed: manual, automatic, online and offline. However, it should be noted that the Directive is "framework legislation" which sets forth minimum standards to be incorporated in the law of each Member State. While the Directive also sets a ceiling in some instances, it does not prohibit divergences among Member State laws.

A key provision of the Directive restricts the transfer of employee and consumer personal information from the EU 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.

In response to the difficulties faced in satisfying the alternative grounds for data transfers provided under the Directive (e.g., ad hoc contracts and model clauses), the U.S. and the EU negotiated and adopted a safe harbor framework ("Safe Harbor") which became effective in July of 2000. Under the Safe Harbor, U.S. companies that voluntarily decide to adhere to the self-regulatory framework will be deemed "adequate" and data transfers from the EU to such companies will be permitted. One of the principal advantages of the Safe Harbor to U.S. companies is that all 25 Member States are bound by the EU adequacy determination.

Every business with employees in a Member State must comply with the Directive and Member State laws implementing the Directive. This means, for example, that a subsidiary (or branch office) of a U.S. company based in the EU may not transfer personal data to its parent or other affiliate (absent an exception discussed below) unless the transferee entity has certified compliance with the U.S. Safe Harbor.

National Implementation and Penalty Assessment

Substantially all countries which were Member States as of the effective date of the Directive have passed laws implementing the Directive: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden and the United Kingdom. The ten countries joining the EU after this date have or are in the process of enacting compliance legislation: Cyprus, Czech Republic, Estonia, Hungary, Latvia, Liechtenstein, Malta, Poland, Slovakia, and Slovenia. However, as the European Commission recognized in its "Report on the Transposition of the Data Protection Directive 95/46/EC" of May 15, 2003, Member State laws governing data transfers out of the EU are complex, and often, contradictory. To reduce the burden of compliance, the Commission's Report urged industry and Member States to harmonize codes of conduct and give greater consideration to voluntary compliance mechanisms.

In addition to the United States, the EU has determined that three countries also provide "adequate" data protection: Argentina, Canada, and Switzerland. The Directive's rules on cross-border data have also heavily influenced developments in other countries. Australia, Brazil, Malaysia, Mexico, South Korea, Taiwan and Thailand, for example, have either adopted or are considering legislation that would impose restrictions on cross-border transfers.

The Directive has spawned a variety of litigation and case developments. In July of 2000, the European Commission took France, Luxembourg, the Netherlands, Germany and Ireland to the European Court of Justice ("ECJ") for failure to implement the personal data protection measures of the Directive. In November of 2003, the ECJ handed down a decision in *Criminal proceeding against Bodil Lindqvist* that clarified the circumstances under which posting of personal data on a website would constitute a "transfer of data" to a third country in violation of Sweden's national data protection law. The decision also established the right of individuals and organizations to challenge national laws on the ground that they go further than prescribed in the Directive.

European Union nations have also assessed millions of dollars in fines for violations of their data protection laws, with the highest to date running about $900,000. Spain has been particularly aggressive, assessing fines against several hundred companies (including Microsoft). Canada has launched a wide spectrum of investigations and found many violations. Thus far, none of the violations have resulted in the civil penalty most likely to cripple the operations of a U.S. multinational: an EU order prohibiting it from exporting its data to the United States. However, it is expected that the volume of enforcement activities and severity of related penalties will increase markedly in the coming months.

Essential Provisions of the Directive

The Directive establishes strict requirements for the processing of personal data. "Processing includes any operations involving personal information , including copying and filing activities. "Sensitive" data may not be processed except under very limited exceptions (e.g., explicit consent, provision of heath care, law enforcement).

Each Member State is required to establish an independent data protection authority ("DPA") to supervise the collection of personal data. An employer that is processing data must register and/or notify the DPA prior to processing any data unless the employer fits within an exemption provided under a Member State law. The registration process includes providing the DPA with information on (i) the purpose of the processing, (ii) the categories of individuals whose data are being processed and types of related data, (iii) the categories of recipients, (iv) proposed transfers to third countries, and (v) security measures.

An employer (referred to in the Directive as a "data controller") must have appropriate legal grounds to process personal information. To meet this "legitimacy" standard, such processing must be "necessary for the achievement of the objective in question rather than merely incidental to its achievement." Legitimacy may be established by several means, including (i) processing necessary for the performance of a contract between the company and the employee; (ii) processing necessary for compliance with legal obligation; (iii) processing necessary for purposes of a legitimate interest; and (iv) processing with employee consent.

Even if an employer's process is legitimized, however, the employee will be entitled in most cases to receive notice about employee data the employer is collecting (both directly and indirectly from other sources), and how the information will be used.

Under the Directive, the employer must institute measures to ensure that personal data is maintained securely and protected against unauthorized disclosure or access. Employees must also be given the right to access and correct such information.

"Unambigious" consent is required for the transfer of personal data within or outside the EU. However, if consent is relied on to legitimize disclosures to third parties within the EU, many Member State laws require that non-consenters opt-out (unless sensitive information is involved). Cross border data transfer, on the other hand, most often requires opt-in or affirmative consent.

U.S. Safe Harbor Framework

The Safe Harbor Framework negotiated between the U.S. and EU specifies that a company seeking the benefits of the Safe Harbor must be subject to the jurisdiction of a governmental body which is empowered to investigate complaints and to obtain relief against unfair and deceptive practices in case of noncompliance. Currently, the Federal Trade Commission and the Department of Transportation are the only U.S. "governmental bodies" which have been recognized by the European Commission. Therefore, only employers subject to the jurisdiction of these two agencies are eligible to join the Safe Harbor. Financial services institutions subject to the jurisdiction of banking agencies and telecommunications carriers subject to the jurisdiction of the Federal Communications Commission are not eligible to join the Safe Harbor at this time.

An eligible organization must publicly declare in its privacy policy statement that it adheres to the Safe Harbor in order to participate. Further, the employer must also self-certify to the U.S. Department of Commerce ("DOC") that it complies with the principles of the Safe Harbor which

apply to both consumer and employee information (FAQ 9 of the DOC's frequently asked questions specifically addresses human resource issues).

While the Safe Harbor parallels the Directive in many respects, there is no requirement for a data controller, registration of databases, or prior approval of data transfers. Similar to the Directive, the Safe Harbor requires an organization to provide employees and/or consumers (i) notice of the purposes for which information about them is being collected and the types of third parties to which information about them is being disclosed as well as of the means for limiting the use and disclosure of information, and (ii) the opportunity to choose (opt-out) when their information may be used for an incompatible purpose or disclosed to a third party other than an agent of the employer. However, the access requirements of the Safe Harbor are far less restrictive and incorporate a "reasonableness" standard not included in the Directive. For example, 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 or persons other than the individual would be violated."

Consistent with the Safe Harbor's self regulatory approach, companies that adhere to the Safe Harbor are required to make a dispute resolution mechanism available to handle the investigation and resolution of individual complaints, as well as procedures for verifying compliance. While these requirements can be satisfied in different ways, most U.S. companies choose to comply by subscribing to a third party privacy seal program (e.g., TRUSTe, Better Business Bureau). It should be noted, however, that even if a mishandling of personal information involving a breach of the Safe Harbor takes place in the U.S. due to the fault of the U.S. data importer, the EU company which transferred the information will remain primarily liable under Member State data protection laws.

Personal Data Transfers to "Inadequate" Countries or U.S. Organizations Not Subscribing to Safe Harbor Framework

The Directive provides several exceptions that permit international transfers of personal information where there is no "adequacy" determination, or to U.S. companies that choose not to subscribe to the Safe Harbor. In general, these exceptions parallel those provided in the Directive for legitimizing data processing in the EU and include situations where (i) the data subject has given unambiguous consent; (ii) the transfer is necessary for the performance of a contract with the individual; (iii) the data exporter has entered into an appropriate contract with the data importer outside the EU, which in most cases requires approval of Member State DPA ("ad hoc contracts"), or (iv) the applicable data transfer agreement incorporates standard clauses that have been approved by the European Commission ("standard clauses"). As discussed below, reliance on these exceptions comes with significant drawbacks.

With respect to the consent exception, some Member States take the position that consent from existing employees is suspect or invalid to legitimize cross border transfer from the EU to third countries. In these particular countries, it may be a risky proposition for employers to rely on opt-in or opt-out consent. Use of employee information transferred on the basis that it is necessary to complete an employment contract is strictly limited to the purposes for which it was transferred (e.g., pay and provide benefits) and broader use is not permissible. While ad hoc

contracts have traditionally served as the legal basis for transferring personal data from Europe, such contracts must now be approved in many cases by a Member State DPA with the potential for significant processing delays and downstream Member State law requirements. Finally, the standard clauses approved by the European Commission contain a variety of onerous requirements (e.g., data subject becomes a third party beneficiary of the agreement, data importer is subject to audit by DPA, Member State law governs agreement, parties agree to jurisdiction of Member State courts) which make this exception unpalatable to most U.S. employers.

Recommendations For Employers

Review Internal Procedures.

· Conduct a comprehensive data protection audit which teams human resource professionals with knowledgeable lawyers;

· Establish procedures and policies to ensure that personal information will be handled accurately and purged when such information is no longer required for the purposes acquired;

· Ensure that employee information is protected against unauthorized disclosure and access;

· If the company has employees in EU Member States, comply with registration requirements and other provisions of national data protection laws.

Catalog Information and Uses.

· Catalog all personal information - employee and consumer – collected and determine how that information is used, to whom it is disclosed and to what countries it is transferred;

· Segregate "sensitive" information for special treatment and handling;

· If personal information is transferred to the United States from an EU organization, clearly ascertain the legal basis for the transfer of such information, e.g., ad hoc contracts, model contracts, consent, and ensure compliance with the chosen basis.