European Union Directive on Data Protection

Introduction

The European Union Directive on Data Protection (the "Directive"), dated October 14, 1995, requires European Union member countries ("Member Countries") to implement national legislation to protect the privacy of individuals. The Directive, which became effective October, 1998, prohibits personal data flows to countries outside of the European Economic Area ("EEA"). Consequently, the Directive affects multi-national organizations doing business in Member Countries insofar as the Directive applies to the "processing" of "personal data," which terms are broadly defined to include any operation performed on any information relating to an identified or identifiable natural person. The transfer of personal data outside of the EEA is allowed only if the individual consents or the recipient of the data employs sufficient safeguards to protect the personal data. Furthermore, there are a number of countries, such as Switzerland, Argentina, and Canada, that are recognized by the European Union as having privacy regimes that are similar to those of other Member Countries and as such are treated as though they are Member Countries. Note, however, that Member Country-specific research is required in determining whether the transfer of personal data is permitted. With regard to the United States, the European Commission has approved a so-called "Safe Harbor" arrangement whereby companies and organizations in the United States commit themselves to comply with a set of data protection principles. The European Commission has held that organizations that comply with the requirements of the Safe Harbor are prima facie considered to have an adequate level of protection to enable transfers of personal data from the EEA. This memorandum summarizes the content of the Directive and the Safe Harbor. Please note, however, that this memorandum does not constitute legal advice and is not intended to substitute for the services of legal counsel.

The Directive

The Directive aims at protecting the fundamental rights and freedoms of persons with respect to the processing of personal data and ensuring the free movement of data between Member Countries. "Personal data" is defined as 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, psychological, economic, cultural or social identity. The Directive, which applies to all processing of data, whether on-line or off-line, manual as well as automatic, stipulates that Member Countries adopt laws that will require the following:

- That personal data be processed fairly and lawfully.
- That the use of personal data be limited to the purpose first identified and to other compatible uses.
- That personal data be kept accurate and up-to-date.
- That the data subject be informed about the circumstances of the data processing at the moment of collection directly from the data subject or at the time of undertaking the recording of personal data and never later than the time when the data are first disclosed.
- That personal data pertaining to race, ethnicity, politics, religion, health, or sexuality not be processed at all unless such processing comes within limited exceptions, such as personal consent.
- That personal data be protected against destruction, loss, alteration, or unauthorized disclosure.

- That organizations processing data appoint "data controllers" who must register with government authorities and notify the authorities before processing any data.
- That Member Countries establish "Data Protection Commissions."
- That the government of an individual Member Country require the processor of the data to provide to the data subject certain information such as:
  - Whether the data subject has rights to see the data;
  - Whether the data subject has rights to correct any information that is inaccurate;
  - Whether the data subject will know the identify of the processor of the data.

The Directive has been implemented in different ways by Member Countries, requiring, in some cases, the consent of the data subject.

The Safe Harbor

The Safe Harbor, which was approved by the European Commission in July, 2000, provides some U.S. organizations with the means of satisfying the "adequacy" requirement under the Directive. The Safe Harbor framework is set forth in a set of safe harbor privacy principles (the "Principles") and 15 frequently asked questions ("FAQs") and answers. Currently, any U.S. organization that is subject to the jurisdiction of the Federal Trade Commission ("FTC"), and the U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation ("DOT"), may participate in the Safe Harbor. Please note, however, that it is still not clear whether the Safe Harbor applies to organizations that are not under FTC jurisdiction, such as financial services, transport, and telecommunications. While the decision by U.S. organizations to enter the Safe Harbor is entirely voluntary, organizations that decide to participate in the Safe Harbor must comply with the Safe Harbor's requirements and publicly declare that they do so. To be assured of Safe Harbor benefits, an organization needs to self-certify annually to the Department of Commerce in writing that it agrees to adhere to the Safe Harbor's requirements, which include elements that parallel the requirements of the Directive (discussed above), such as notice, choice, access, and enforcement (see below). It must also state in its published privacy policy statement that it adheres to the Safe Harbor. The Department of Commerce maintains a list of all organizations that file self-certification letters and makes both the list and the self-certification letters publicly available. A European Union organization can ensure that it is sending information to a U.S. organization participating in the Safe Harbor by viewing the public list of Safe Harbor organizations posted on the Department of Commerce's web site. The Department of Commerce lists the Safe Harbor requirements as follows:

Notice: An organization must inform individuals of the purposes for which it collects information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.

Choice: An organization must offer individuals the opportunity to choose (a) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual or (b) to opt out. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

Safe Harbor Sensitive Information Principle: For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), an individual must be given affirmative or explicit (opt-in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt-in choice.

Onward Transfer: An organization may only disclose personal information to third parties consistent with the principles of notice and choice.

Security: Organizations creating, maintaining, using or disseminating personal information must take reasonable measures to assure its reliability for its intended use and take reasonable precautions to protect it from loss, misuse or unauthorized access, disclosure, alteration or destruction.

Data Integrity: An organization may only process personal information relevant to the purposes for which it has been gathered.

Access: Individuals must have reasonable access to personal information that an organization holds about them, and be able to correct or amend that information where it is inaccurate.

Enforcement: Effective privacy protection must include mechanisms for assuring compliance with the Safe Harbor Principles, recourse for individuals affected by noncompliance with the Principles, and consequences for the organization when the Principles are not followed.

Contact Information

If you have any questions or would like to learn more about the Directive or the Safe Harbor, please contact your usual legal advisor at Ropes & Gray.