Order Code RS20823
Updated August 6, 2002

The EU-U.S. "Safe Harbor" Agreement on Personal Data Privacy

Martin A. Weiss
Analyst in International Trade and Finance
Foreign Affairs, Defense, and Trade Division

Summary

The European Union (EU) Data Privacy Directive adopted by the European Parliament and Council on October 24, 1995 prevents EU-based organizations, public and private, from transferring personal data to countries where the legal protections for personal data are not deemed "adequate." This Directive, intended to harmonize national European privacy policies, allowed EU member countries three years to implement the Directive. To prevent the interruption of data transfers, the U.S. Department of Commerce (DOC) negotiated the "Safe Harbor" Agreement with the EU. While the EU has recently stated that all elements of the agreement are in place, "Safe Harbor" raises many significant issues of interest to Congress. These include the extraterritorial application of EU law, non-tariff barriers, business costs, consumer protection, as well as enforcement and dispute settlement.

Background[1]

On October 24, 1995, the European Union (EU) agreed upon Directive 95/46 EC to harmonize differing national legislation on data privacy protection.[2] The Directive creates a legally binding obligation on each EU member state to implement domestic legislation conforming to a unified set of standards. It is expected to facilitate information flows within the EU, strengthen the EU's internal market and foster the development of an information-based economy. This Directive was supplemented two years later by Directive 97/66/EC which concerned the handling and privacy of personal data in the telecommunications industry.

[1] This report was originally prepared by Patricia A. Wertman, Specialist in International Trade and Finance, Foreign Affairs, Defense and Trade Division.

[2] This and other official EU documents relating to data protection can be found at [http://europa.eu.int/comm/internal_market/en/dataprot/].

The Directive applies to all organizations, public and private, operating in the EU, including affiliates of U.S. corporations. It covers the processing of all personal data, whether done automatically or manually. There is no exception for public records, such as telephone directory listings. Only information compiled for private, personal household use is excluded. Under the Directive, data may be collected and used only for specified, explicit, and legitimate purposes. Security and accuracy must be guaranteed. Individuals have not only the right to access and the right to correct errors, but also to remedial measures and compensation, if necessary. The transfer of data to third parties may occur only under similarly strict requirements. More stringent rules apply to the processing of sensitive data, including data relating to race; ethnic origin; political, religious, or philosophical beliefs; and health status or sex life. The Directive also requires the creation of "Data Protection Agencies" (DPAs) in each of the fifteen EU member states; registration of data bases with these authorities, and, sometimes, prior DPA approval before organizations or firms may begin data processing.

The transfer of personal data to any nation outside the EU that does not meet the EU test of "adequacy" with regard to privacy protection is prohibited. According to the EU, privacy protection in the United States may fail this test. The Directive, thus, potentially threatens to disrupt or, in some limited cases, even prevent the transfer of data between the EU and the United States.

Rationale for the Agreement

Europe and the United States have fundamentally different attitudes towards the protection of personal data. The right to privacy is a fundamental human right recognized both in the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of European Community laws. With regards to personal information, Europeans are more trusting of governments than the private sector. It follows that European governments have turned to legislation to regulate the flow of personal information.

By contrast, the United States has adopted a sector-by-sector approach through a mix of legislation, regulation, and industry self-regulation, such as the federal rules applicable to medical records. Moreover, U.S. firms tend to view personal data as a valuable commercial asset rather than as an individual asset. Until recently, it had been left to the marketplace to establish privacy principles on a sector-by-sector basis. Congress has increased its involvement in the privacy area most notably with the enactment of financial privacy legislation in 1999, children's online privacy legislation in 1998, and the consideration of online privacy legislation in the 107th Congress.

To prevent the stoppage of data transfers from the EU to the U.S., the U.S. Department of Commerce (DOC) negotiated the "Safe Harbor" agreement with the EU. The agreement gained EU Commission approval in July 2000, and become operational on November 1, 2000. The DOC "Safe Harbor" website [http://www.export.gov/safeharbor/] provides information to U.S. organizations and makes available an up-to-date list of U.S. organizations that adhere to the "Safe Harbor" principles (currently 217).

The "Safe Harbor" was created to permit U.S. companies that voluntarily adhere to the principles to continue cross-border data transfers with EU member states. The

principles are designed to serve as guidance to U.S. organizations seeking to comply with the "adequacy" requirement of the directive, and would provide organizations within the "Safe Harbor" a presumption of adequacy and data transfers from member states of the European Union could continue. Organizations would come into the "Safe Harbor" by self-certifying that they adhere to these privacy principles.

In a February 13, 2002 working paper (SEC (2002) 196), the EU Commission noted that all elements of the "Safe Harbor" agreement are in place. Current European concerns address the level of transparency needed to discern an individual firm's commitment to the agreement and the fact that the dispute settlement mechanisms have not been tested. Other European and domestic concerns include the vagueness of "adequacy" determination, the lack of agreement on transfer of personal information in financial services, the possible disputed legality of FTC enforcement, and the actual willingness of the FTC to prosecute US firms on behalf of the EU.

Basics of the "Safe Harbor" Framework

In addition to the EU Privacy Directive itself, the "Safe Harbor" framework encompasses seven basic principles, fifteen "frequently asked questions" (FAQs), the EU Commission's "adequacy" decision, an exchange of letters between the DOC and the EU Commission, and an exchange of letters between the United States Departments of Transportation (DOT) and Federal Trade Commission (FTC) and the EU Commission . These are all available on the DOC web site. The seven basic principles, in edited and abridged form, are:[3]

- **Notice**: An organization must inform individuals about the purposes for which it collects and uses information, how to contact the organization with inquiries or complaints, and the types of third parties to which it discloses the information.

- **Choice**: An organization must offer individuals the opportunity to choose (**opt-out**) whether their personal information is (a) to be disclosed to a third party or (b) 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.

  For **sensitive information**, individuals must explicitly **opt-in** when personal data is to be transferred to a third party or used for a purpose other than the one for which it was originally collected or subsequently authorized. Sensitive information includes information about medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information regarding the individual's sex life.

- **Onward Transfer**: In transferring information to a third party, organizations must apply the Notice and Choice Principles. Third parties acting as agents must provide the same level of privacy protection either by subscribing to "Safe Harbor," adhering to the Directive or another adequacy finding, or entering into a contract that specifies equivalent privacy protections.

- **Security**: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

- **Data Integrity**: Personal information must be relevant for the purposes for which it is to be used. . . . an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

- **Access**: Individuals must have access to the information about them that an organization holds and must be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense would disproportionate to the risks to the individual's privacy or where the rights of others would be violated.

- **Enforcement**: Effective privacy protection must include mechanisms for verifying compliance; readily available and affordable independent recourse mechanisms in cases of non-compliance; and consequences for the organization when the Principles are not followed. Sanctions must be rigorous enough to ensure compliance.

Eligibility and Enforcement

While joining "Safe Harbor" is voluntary, any organization that receives data from the EU must comply with the Privacy Directive. Participation in the "Safe Harbor"is open to any U.S. organization that is subject to regulation by the Federal Trade Commission (FTC), which enforces a variety of consumer protection laws, including those related to unfair and deceptive practices, and to United States air carriers and ticket agents that are subject to regulation by the Department of Transportation (DOT). To qualify, organizations must self-certify annually in a letter to the DOC that they adhere to the safe harbor principles.

Enforcement of the "Safe Harbor" Agreement is to be undertaken both by the private sector and by federal and state authorities enforcing unfair and deceptive practices laws. Private sector enforcement has three components: verification, dispute resolution, and remedies. Persistent failure to comply will result in withdrawal of "Safe Harbor" status, a fact that will be listed on the "Safe Harbor" web site, and also, potentially, by regulatory action. A cause of congressional concern is the questioned legality of FTC enforcement. During the "Safe Harbor" negotiations, the FTC guaranteed that it would investigate cases upon European request, but according to some, the FTC might not have enforcement authority.[4]

Organizations that do not fall under the jurisdiction of the FTC and the DOT are not eligible for "Safe Harbor." Notably, this includes U.S. financial firms and telecommunications carriers. In particular, the EU does not consider that the Fair Credit Reporting Act (P.L. 91-508; 15 U.S.C. 1681 et seq.) or the recently enacted Financial Services Modernization Act (P.L. 106-102, popularly known as the Gramm-Leach-Bliley Act) provide adequate privacy protections. As a result, negotiations between the United

---

[4] Reidenberg, Joel R. "E-Commerce and Trans-Atlantic Privacy." *Houston Law Review*, Fall, 2001. pp. 719-738.

States and the EU to achieve an agreement covering the financial sector continue. While negotiations regarding data transfers in the financial services are still taking place, a"standstill" on any EU action against data transfers from the EU to the U.S. is in effect. The U.S. government and private financial institutions have called upon the EU to grant an "adequacy" determination to financial services firms. They argue that privacy legislation such as the Fair Credit Reporting Act, the Financial Services Modernization Act, and numerous state laws confer more than "adequate" protection of data privacy in the financial services industry.[5]

Issues for Congress

"Safe Harbor" is clearly intended to facilitate trans-Atlantic data exchange and, hence, trans-Atlantic commerce, both on-line and off. Nevertheless, it raises a number of policy concerns that may be of interest to Congress[6]:

- **Extraterritoriality**: Article 25 of the EU Directive allows for individual analysis of third-party countries that transfer personal information from Europe and gives the EU the right to halt the flow of information if they determine that the third parties do not have "adequate" privacy protection. A determination of "adequacy" can be made by any EU member. This presents two specific concerns. First, the Directive extends EU law beyond EU boundaries, not just to the US, but to any nation with which EU organizations are likely to exchange personal information. Second, some analysts are concerned that since the definition of "adequacy" is left vague, the EU and its member states, could selectively define "adequate" protection, thus using data privacy as a form of non-tariff barrier.[7]

- **Consumer Protection**: In recent years, the privacy issue has achieved heightened importance among consumers, particularly those using the Internet. Consumer advocates in Europe worry that "Safe Harbor" falls short of European data protection laws. Some Europeans are concerned whether EU citizens who feel that their privacy rights are being violated will have the right to sue in United States courts. Domestically, some are concerned that U.S. firms will be extending greater protection to Europeans than to our own citizens. The effectiveness of business-backed self-regulatory privacy programs such as BBBOnline and TRUSTe has also been questioned. Balancing consumer and business interests in a workable regulatory framework, however, might provide a competitive advantage, building consumer confidence and furthering the development of e-commerce.

- **Relationship to the U.S. Law**: While the "Safe Harbor" framework might be seen as accommodating international realities, FTC and DOT enforcement could give

---

[5] Yerkey, Gary G. "U.S., EU Move to Close Gap in Dispute Over Data Privacy but No Resolution in Sight." *International Trade Reporter*, Vol. 19, No. 30, July 25, 2002.

[6] See also, United States Library of Congress. Congressional Research Service. *Electronic Commerce: An Introduction*, by Glenn J. McLoughlin, CRS Report RS20426; and *Internet Privacy: Overview And Pending Legislation*, by Marcia S. Smith, CRS Report RL31408.

[7] See Solveig Singleton, Privacy As A Trade Issue: Guidelines for United States Trade Negotiators. *The Heritage Foundation.* March 18, 2002.

"Safe Harbor" the force of law. The U.S. Congress did not participate in its formulation, but must contend with private sector concerns regarding its requirements. Moreover, in extending EU law on privacy to U.S. organizations, it affects the domestic debate on privacy issues. The EU Directive has been seen by some as a model of data privacy protection and reportedly played a role in the January 1, 2001 implementation of a new privacy law in Canada.[8] Some suggest that as the Internet strengthens its global presence, and other countries, such as those in Europe, take an active position in creating standards for this new medium, the importance of U.S. standards and rules will likely diminish.

- **Compliance**: Compliance within the EU itself is uneven. The EU Commission took legal action against six states – Denmark, France, Germany, Ireland, Luxembourg, and the Netherlands for failure to comply with the Directive. According to one source, Luxembourg has been condemned by the Court for its non-compliance. Ireland has a Bill in Parliament, but it has not been adopted yet. The cases against Denmark, France, Germany, and the Netherlands have since been dropped.

- **Encryption**: The privacy of data in the computer age is often achieved by using encryption technology. Thus, US policy on the export of encryption technology shadows this issue. Even after the July 2000 liberalization, allowing export of encryption products of any strength to both government and private sector entities in the EU, export of encryption technology remains subject to certain controls.

- **Market Segmentation**: The Directive may cause firms to segregate their European operations, especially their data processing, from those in the United States and elsewhere. This compliance could require expensive organizational changes. Data subject to the Directive may have to be maintained and processed separately and a series of notices and permissions are required. Affiliates and subsidiaries might be considered "third parties,"ensuing that data derived by a European subsidiary might not be transferrable to its U.S. parent. Restrictions apply as long as the data is held, that is, *in perpetuity*.

---

[8] See Pritchard, Timothy. "Canada Strengthens Internet Privacy." *New York Times*, December 23, 2000, p. B2.