Global Information Assurance Certification Paper

Entering a Safe Harbor: What do U.S. businesses need to know?

Noelle Hardy
January 31, 2001

Abstract

The U.S. and European Union (EU) have historically taken differing approaches to protecting the privacy of their citizens and the free movement of personal data. The EU has moved toward comprehensive legislation with the adoption of the Directive on Data Protection (Directive 95/46/EC), while the U.S. relies on an approach based heavily on industry and self regulation, combining some federal and state legislation where needed. Directive 95/46/EC prohibits the transfer of personal data from EU members to non EU nations except in those cases where the non EU nation has complied with the European "adequacy" standard for privacy protection. As a nation, the U.S.'s current approach to privacy protection is not considered to be adequate by European standards.

Recognizing the potential impact on trade with EU member nations, the U.S. Department of Commerce negotiated with the EU to develop the safe harbor provisions, which provide individual U.S. organizations with clear mechanisms for addressing this situation. Under the safe harbor provisions, organizations are provided a means by which they can assert adequate privacy practices, thus avoiding potential interruptions in flow of critical business data or the potential prosecution by European authorities under European privacy laws.

European Union Directive on Data Protection

The European Commission's Directive on Data Protection (Directive 95/46/EC) went into effect in October 1998. The Directive enables the free movement of personal data between the 15 European Union member states[1] by harmonizing national data protection laws. The differences between the national data protection laws of the various member states were seen as an obstacle that could seriously impede the future growth of the information society.

The Directive is designed to protect privacy of individuals by legislating the manner in which personal data is processed, where processing includes operations such as collection, storage, disclosure, etc. Personal data is limited to information that relates to any identified person (e.g., names, birth dates, unique identifiers, pictures, addresses, etc.) as well as information that could reasonably lead to the identification of an unknown person.

The Directive places obligations on the data controllers (i.e., individuals determining the purposes and means of processing) to collect personal data only for specified, legitimate purposes and to use it accordingly. Data controllers are advised to keep data in a form

[1] The fifteen European countries that belong to the EU are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

which permits identification of individuals for no longer than it is necessary. Under the Directive, data subjects have the right to access their personal data, the right to know where the data originated, the right to have inaccurate data rectified, a right of recourse in the event of unlawful processing and the right to withhold permission to use their data in certain circumstances. Sensitive data, such as an individual's ethnic or racial origin, political or religious beliefs, trade union membership or data concerning medical history or sexual orientation, can only be processed with the explicit consent of the individual. Situations were there is a critical public interest are considered exceptions, however, alternative safeguards must be established.

In order to ensure the continued protection of personal data, the Directive prohibits the transfer of such data to non European Union nations that do not meet the European "adequacy" standard for privacy protection. Certain limited exceptions are supported by the Directive where the individual has given their unambiguous consent for the transfer or where the transfer is in response to actions taken by the individual (e.g., job application) or if the transfer is perceived as protecting the vital interests of the individual. Transfers can also be allowed in cases where contractual provisions have been developed that bind the receiver of the data to providing the same safeguards as enumerated within the Directive.

A Safe Harbor: Program Overview

Implications of the EU Directive for multinational organizations could be significant, resulting in the disruption of business operations. Concerned about the potential impact on U.S. - EU trade, which in 1999 amounted to $350 billion, the U.S. Department of Commerce, in consultation with the European Commission, has established a "safe harbor" framework for U.S. organizations. Under this agreement, U.S. companies can continue to receive personal data from all 15 EU member states, as long as they subscribe to a set of privacy principles associated with the safe harbor provision. The safe harbor principles were developed to more closely reflect the U.S. approach to privacy while also meeting the European Commission adequacy standards.

The safe harbor provisions were approved by the EU in July, 2000 and went into effect in the U.S. in November 1, 2000. This program is applicable to any U.S. organization receiving or storing personally identifiable data about citizens from any of the European Union countries. In order to participate organizations will need to either adopt or modify current data protection practices so they are compliant the seven safe harbor principles. Then, on an annual basis, the organization will be required to self certify to the Department of Commerce that it agrees to adhere to the safe harbor requirements. The organization's published privacy policy must also state that it adheres to the safe harbor privacy principles. A list of the safe harbor organizations will be maintained by the Department of Commerce at their website (www.export.gov/safeharbor).

Enforcement will rely heavily on private sector self regulation, with approved government agencies providing back up through the enforcement of federal and state laws prohibiting unfair and deceptive acts. In order for the safe harbor provisions to be

successful, organizations failing to comply with self regulation must be actionable by approved government bodies. The Federal Trade Commission and the Department of Transportation have both pledged to enforce actions against organizations failing to live up to claims of compliance. For example, the Federal Trade Commission Act makes it illegal in the U.S. to make representations to consumers or to commit deceptive acts that are likely to mislead reasonable consumers. As such, the FTC has the ability to seek civil penalties up to $12,000 per day for violations and instances of misrepresentation by organizations failing to abide by prior stated commitments to the safe harbor privacy principles.

At this point in time, only those organizations falling under the jurisdiction of the FTC or U.S. air carriers and ticket agents subject to the jurisdiction of the DOT may participate in the safe harbor program. This currently excludes the financial services and telecommunications sectors. Discussions specifically regarding financial services have been placed on hold pending guidance regarding the implementation of the Gramm-Leach-Bliley Act of 1999.[2] It is expected that additional government agencies will agree to enforce the program provisions thus opening the program to other industries.

Participation in the safe harbor is completely voluntary. Organizations may choose to explore other alternatives such as negotiating directly with European authorities regarding the transfer of information. Organizations can also chose to change business processes such that personal data is processed within EU member state borders or made anonymous either by stripping relevant fields or through aggregation. The safe harbor principles are thought to offer a more flexible and simpler means of demonstrating compliance, which will particularly benefit small to medium enterprises.

Safe Harbor Principles

Compliant privacy policies must address the seven safe harbor privacy principles as well as any relevant points covered in the safe harbor frequently asked questions (FAQs). In addition, the privacy policy must document actual and planned information handling practices, and clearly state that the organization is compliant with the safe harbor privacy principles.

The FAQs provide guidance for implementing the privacy provisions with respect to specific industries or types of data. In addition, exceptions to the provisions are discussed. For instance, the FAQs address journalistic exceptions, the issue of secondary liability, and requirements for handling data such as human resources information, travel information, and information relating to the development of pharmaceutical and medical products. Other FAQs provide elaboration on meeting particular aspects of the safe harbor principles such as verification and enforcement.

A high level overview of the safe harbor principles is as follows:

[2] The Gramm-Leach-Bliley Act requires banking agencies to establish appropriate standards for financial institutions relating to the administrative, technical and physical safeguards of customer records and information.

- **Notice** – Organizations must inform individuals as to the purposes for which information about them is being collected and used, and the types of third parties to whom the organization may disclose information. Individuals must be informed how they can contact the organization with inquires or complaints as well as the choices they have with respect to limiting the use and disclosure of information about them.
- **Choice** – Individuals must be provided the opportunity to "opt out" of allowing their information to be disclosed to a third party or to be used for a purpose incompatible with the purpose for which it was originally collected.
- **Safe Harbor Sensitive Information Principle** – For sensitive personal information, such as that specifying medical conditions, racial or ethnic origin, political opinions, religious beliefs, or sexual orientation, individuals must explicitly "opt in" before such information can be disclosed to a third party or be used in a manner other than for which it was originally collected.
- **Onward Transfer** – Prior to disclosing information to a third party, the organization must ensure that the third party provides the same level of privacy protection as required by the safe harbor principles. Having done this, the organization will not be held responsible should the third party process the data in a manner contrary to the safe harbor privacy principles.
- **Security** – Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
- **Data Integrity** – Organizations must take reasonable steps to ensure that data is accurate, complete, current, relevant, and reliable for its intended use.
- **Access** – Organizations must provide individuals with access to personal information collected about them. Individuals must be allowed to correct, amend, or delete such information if it is inaccurate. Exceptions to this principle may be allowed where the burden or expense of providing such access is considered disproportionate to the risks to the individual's privacy.
- **Enforcement** – Organizations must define procedures and mechanisms for assuring compliance with the principles. These mechanisms must also include a means by which complaints and disputes raised will be investigated and resolved, and obligations whereby sanctions will be applied should the organization fail to be compliant.

A statement of verification must either be signed by a corporate officer or an independent reviewer indicating that the organization's published privacy policy is accurate, comprehensive, prominently displayed, completely implemented, and in compliance with the safe harbor principles. Organizations must also clearly advertise how complaints from individuals who feel their privacy may have been violated will be investigated and resolved. Organizations can choose to engage a third party dispute resolution mechanism by complying with one of the private sector seal programs being developed by entities such as BBBOnline, Truste, AICPA WebTrust, and the Direct Marketing Association. Organizations may also choose to cooperate with either U.S. government supervisory authorities or data protection authorities located in Europe. Regardless of the

dispute resolution system chosen, the safe harbor provisions require that potential sanctions applied through the system must be severe enough to ensure compliance by the organization. For instance, they should include public notification of findings of non-compliance as well as possible suspension from the safe harbor program in some cases.

Organizations may choose to withdraw from the program at any time by notifying the Department of Commerce. Failure to comply with safe harbor provisions without officially withdrawing from the program could be interrupted as a misrepresentation with respect to asserted compliance. Such misrepresentations could be actionable under the False Statements Act (18 U.S.C. 1001).

Private Sector Seal Programs

Truste, a non profit organization which currently licenses its existing seal to approximately 2,000 Web sites, announced on November 1, 2000 that they would be launching a safe harbor certification program. Under the program Truste would certify that an organization's data gathering and handling practices and policies are in compliance with safe harbor provisions. A quarterly monitoring program will be implemented to support enforcement of the provisions and ensure ongoing compliance. As an additional service, Truste will handle dispute resolution for organization's participating under its certification program. The dispute resolution can cover both online and offline cases. Such private sector seal programs are welcomed and supported by the Department of Commerce. Additional information about the Truste program and a model compliant privacy statement can be found at their website http://www.truste.com. Similar programs are under development by BBBOnline, AICPA WebTrust, and the Direct Marketing Association.

Conclusions

While increased reliance on the Internet has allowed for significant growth in international e-commerce, conducting business around the globe introduces many issues that are not solved strictly by technology. In order to successfully maximize international e-commerce opportunities, organizations must be sensitive to the differences within specific countries with respect to consumer protection and privacy laws.

The European Commission Directive on Data Protection is of particular interest to organizations seeking to conduct business within any of the 15 European Union member states. In an effort to protect the personal information of European Union citizens, the directive legislates that personal information may only be transferred to non European Union nations where the receiving nation has implemented privacy protections deemed adequate under the provisions of the directive. U.S. companies choosing to comply with the safe harbor provisions would be allowed to continue to receive and handle personal information regarding citizens from European Union nations.

To date, adoption of the Safe Harbor provisions has been slow. As of January 5, 2001 only 12 companies have joined the safe harbor program. In an effort to raise awareness about the program and encourage participation, the Department of Commerce is partnering with the Software and Information Association (SIIA), the U.S. Council for International Business, and Morrison & Foerster to offer the Safe Harbor Business Implementation Forum. The forum is being offered early this spring in California, Washington D.C., New York, and Dallas. The focus of the event is to raise awareness among industry representatives regarding the new U.S.-EU Safe Harbor agreement and provide guidance for developing corporate data privacy policies. For more information see http://www.trensreport.net/events/calendar/events.asp

References

U.S. Department of Commerce Export Portal: Safe Harbor.
URL: http://www.export.gov/safeharbor.

Europa Portal: European Commission on Data Protection.
URL: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.html

Sykes, Rebecca. "EU Privacy law looms, enforcement uncertain". InfoWorld Electric. 22 October 1998. URL: http://www.idg.net/crd_data_32903.html

"U.S. rolls out EU privacy program.". ZDNet IT Resource Center. 5 January 2001. URL: http://www.zdnet.com/enterprise/stories/main/0,10228,2671183,00.html

Johnston, Margret. "Commerce Department tries to boost 'safe harbor' adoption". IDG News Service – Computerworld. 5 January 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO55924,00.html

"An International Survey of Privacy Laws and Practice." Global Internet Liberty Campaign. URL: http://www.gilc.org/privacy/survey/

SIIA Press Release. "SIIA Joins U.S. Secretary of Commerce Norman Mineta to Brief Industry on U.S.-EU Privacy 'Safe Harbor' Agreement." 4 January 2001. URL: http://www.siia.net/sharedcontent/press/2001/1-4-01.html

Truste.com. URL: http://www.truste.com