European Union (EU) Data Protection Directive of 1995
Frequently Asked Questions

Rebecca Herold, CISM, CISSP, CISA, FLMI

NOTE: The following article was published in the Computer Security Institute (www.gocsi.com) May 2002 issue of the Alert newsletter.

Preface

What is the European Union (EU) Data Protection Directive?

The Directive was established to provide a regulatory framework to guarantee secure and free movement of personal data across the national borders of the EU member countries, in addition to setting a baseline of security around personal information wherever it is stored, transmitted or processed. The directive is explained more fully in the following sections of this document.

What does the EU Data Protection Directive mean to companies?

Similar to recent U.S. privacy-related regulations and laws, the EU Data Protection Directive places some very specific information-handling requirements on the data any organization wants or needs to process in one of the EU countries. The U.S. economy is quickly becoming a global economy, with an almost exponential growth in the number of U.S.-based organizations doing business in EU countries. These U.S. organizations **must** meet the requirements of the EU Data Protection Directive to continue doing business if it involves sharing and/or processing data with these countries (which most do.) These organizations will need 1) an understanding of the EU Data Protection Directive, 2) to determine what they must do to meet the requirements, and 3) to implement the requirements.

A. What countries are included in the EU?

The European Union (EU) is a union of fifteen independent states based on the European Communities and founded to enhance political, economic and social co-operation. Formerly known as European Community (EC) or European Economic Community (EEC).

Date of foundation: 1st November, 1993. New members since 1st January, 1995: Austria, Finland, Sweden.

Current European Union Member states:

1. Austria
2. Belgium
3. Denmark
4. Finland
5. France
6. Germany
7. Greece
8. Ireland
9. Italy
10. Luxembourg
11. Netherlands
12. Portugal
13. Spain
14. Sweden
15. United Kingdom of Great Britain and Northern Ireland

B. What are the general requirements of the EU Data Protection Directive?

The full title of the Directive is:
Directive 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The Directive contains 33 articles in 8 chapters. The Directive went into effect in October, 1998.

At a very high level, the six basic tenants of the Directive include the following:

1. NOTICE: An individual has the right to know that the collection of personal data will exist. The personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."
2. CHOICE: An individual has the right to choose not to have the personal data collected.
3. USE: An individual has the right to know how personal data will be used and to restrict its use. Personal data may only be used for "legitimate processing" as described by the Directive details.
4. SECURITY: An individual has the right to know the extent to which the personal data will be protected. Organizations must "implement appropriate technical and organizational measures to protect personal data. The measures must be "appropriate to the risks represented by the processing and the nature of the data be protected."
5. CORRECTION: An individual has the right to challenge the accuracy of the data and to provide corrected information. Personal data collected and maintained by organizations be up to date and reasonable steps must be taken to ensure that inaccurate or incomplete data is corrected.
6. ENFORCEMENT: An individual has the right to seek legal relief through appropriate channels to protect privacy rights.

C. What is considered personal data under the EU Data Protection Directive?

The personal data that the Directive covers includes information relating to 'an identifiable person'. This includes information about a natural person directly identified by an identification number or indirectly with one or more facts that relate to his 'physical, physiological, mental, economic, cultural, or social identity'. A very broad scope indeed!

Sensitive data is an important subset of personal data. Sensitive data is that which reveals racial or ethnic origin, political opinions, religious beliefs, trade union membership, health or sex life details. This information is regarded as sensitive because it could expose the data subject to discrimination as well as infringe on the very fundamentals of privacy. Health information as defined by this article would include past or present information on physical or mental state as well as any abuse of drugs or alcohol.

The Directive recognizes that sensitive information may have to be processed under certain conditions, and therefore establishes exceptions that provide for the processing of sensitive data under specific conditions.

D. Is this the same as the UK's Data Protection Act of 1998?

No. Each member of the EU has, or is in the process of, drafting their own country's privacy legislation to meet the requirements of the EU Data Protection Directive. The UK Data Protection Act is their effort at becoming compliant with the EU Directive.

E. How does this affect EU organizations, or any other non-U.S. organization?

This affects ANY company/organization that wants/needs to move personal data across the borders (into or out of) of any EU country. This is a much broader scope than the U.S. privacy initiatives, such as GLB and HIPAA, with which most of you are probably more familiar. The EU Directive requirements must be met by any company wishing to move information across EU member country borders.

F. How does this affect USA organizations?

The U.S.A. is under the same obligations as previously described. However, because the U.S. has to date promoted self-governance by organizations for more privacy-related information handling issues, the U.S.A. organizations will probably feel the effects much more significantly. With the

expansion of large numbers of U.S.A. companies to EU countries in recent years, it is highly likely many existing information processing systems and management practices will need to be dramatically changed to come into compliance with the EU Directive. These companies will not have a choice. If they want to continue to do business within the EU Countries and move data across their borders they are going to have to make changes if they are not currently in compliance.

If a company is not in compliance, basically any of Europe's 492 million citizens can make a claim of abuse of personal data against the company and pursue the claim through to the European Court of Justice. Accompanying this process, enterprise contracts with the EU country can be suspended, injunctions can be made against the company's dataflows with the EU location(s), and EU citizens can claim compensation. This is an issue U.S.A. companies must take seriously.

G. What is Safe Harbor, and how does it apply to the EU Directive?

To help bridge the differences between the way the U.S.A. government approaches privacy issues and the EU Directive, the U.S. Department of Commerce consulted with the European Commission and developed a "safe harbor" framework that was approved by the EU earlier this year. The Safe Harbor provides a privacy compliance framework and a way for U.S.A. organizations to avoid experiencing interruptions in their business dealings with the EU, or facing prosecution by the European authorities under European privacy laws. Certifying a U.S.A. organization to the Safe Harbor requirements will assure that EU entities know that the organization provides "adequate" privacy protection as required by the EU Directive. Basically the Safe Harbor framework provides a simpler and cheaper means of complying with the privacy adequacy requirements of the EU Directive. This would significantly benefit small and medium organizations in particular.

H. Who is Eligible to Participate in Safe Harbor?

A USA organization must be subject to the jurisdiction of either the Federal Trade Commission (FTC) or the U.S. Department of Transportation (DoT) to be eligible for Safe Harbor. DoT jurisdiction applies to air carriers and ticket agents, while FTC jurisdiction applies to most remaining sectors.

However, FTC jurisdiction does not currently extend to some financial services (namely banks, insurance and credit unions), telecommunications common carriers, meat packers and not-for-profits. (See sections 4 and 5 of the FTC Act). Therefore, those sectors are currently ineligible for Safe Harbor. In certain circumstances, it is possible for a "financial service" to be eligible for Safe Harbor if that organization is not engaging in banking, insurance or credit union activities.

According to FTC representatives in February, 2002, the Treasury Department plans to resume negotiations with the European Commission on the issue of U.S. financial services vis-a-vis the EU directive. In addition, they hope to engage the Federal Communications Commission concerning their potential role in Safe Harbor for common carriers. So, at this time, financial services, meat packers and not-for-profits will need to meet all EU directives on a case-by-case basis with each EU country as necessary for their business purposes.

I. Should Eligible USA organizations "join" Safe Harbor?

This depends on if the USA organization needs to transfer information considered personal data across EU country borders. A review as outlined in item M will help determine this. If so, there are several benefits to becoming Safe Harbor certified:

1. All 15 EU states are bound by the European Commission's finding of privacy protection adequacy as stipulated by Safe Harbor certification.
2. Companies participating in Safe Harbor will be considered to have adequate privacy protections and data flows to those companies can continue.
3. EU member state requirements for prior approval of data transfers will either be waived, or approval will automatically be granted.
4. Claims brought against U.S.A. companies by European citizens will be heard in the U.S. subject to limited exceptions.

J. What are the steps USA organizations must take to be Safe Harbor certified?

U.S.A. organizations must comply with seven principles that generally require the following:

1. **Notice:** Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can 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 for limiting its use and disclosure.
2. **Choice:** Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.
3. **Onward Transfer** (Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.
4. **Access:** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate 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.
5. **Security:** Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
6. **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.
7. **Enforcement:** In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

Enforcement of these requirements will be carried out primarily by the private sector. Private sector self-regulation and enforcement will be backed up as needed by government enforcement of the federal and state unfair and deceptive statutes.

K. What companies have signed the Safe Harbor agreement?

On August 16, 2001, eighty-eight (88) U.S. companies had signed the agreement and pledged to have met the Safe Harbor requirements. As of March 23, 2002, this number had risen 100% to one hundred seventy-six (176) U.S. companies. This number is subject to change at any time as new companies sign the agreement, and as existing companies choose to drop out of the Safe Harbor program (none to date have dropped off to my knowledge.) The current list can be found at:
http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

L. Have any lawsuits resulted from noncompliance with the EU Data Protection Directive?

Yes, citizens of the EU countries, and EU-based organizations, have taken organizations to court to address noncompliance. The following is just an example of such cases.

1. In 1998 Sweden's privacy watchdog, Anitha Bondestam, instructed American Airlines (AA) to delete all health and medical details on Swedish citizens after each flight unless explicit consent from them could be obtained. These details (allergies, asthma notification, dietary needs, disabled access, etc.) are routinely collect by AA at the point of booking. Bondestam's order meant that AA would be unable to transmit this information to the SABRE central reservation system in the U.S. AA appealed to the Country Administrative Court in Sweden. The court was unconvinced by AA's argument that the practice was impractical and people would not want to repeat providing this information for every flight. AA appealed again, lost again, and the case went before Sweden's national Supreme Court. During this time all export and processing of medical data to the reservation system has been banned.
2. In 1999 Microsoft paid $60,000 to settle charges brought by Spain that Microsoft didn't "clearly and conspicuously" disclose to Spanish consumers what happens to personal data when they register for Windows.

M. What can companies do to help determine if they need to comply with the EU Directive, and to determine what steps to take to come into compliance with the EU Directive?

At a very high level…

(1) Identify the organization's potential for current processing of EU personal data;
   (a) If so, identify the personal data
   (b) Determine purposes for the personal data
   (c) Determine validity of personal data
   (d) Document current personal data processing practices, procedures and policies
(2) Perform gap analysis of current personal data processing procedures and practices
(3) Deliver gap analysis report and senior management briefing explaining the issues and management's roles in addressing the issues.
(4) If a U.S.A. organization, determine if Safe Harbor certification should be pursued. If so, assist the organization with the Safe Harbor application.
(5) Develop and implement appropriate policies and procedures for processing and handling the personal data that will comply with the EU Directive.
(6) Develop and deliver a corporate awareness program for staff, targeting those areas that handle or process personal data.
(7) Yearly audit EU Directive compliance.

Rebecca Herold, CISSP, CISM, CISA, FLMI is an independent information security, privacy and compliance consultant, author and instructor. She can be reached at rebeccaherold@rebeccaherold.com or 515-491-1564. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, created "The Privacy Papers," co-authored "The Practical Guide to HIPAA Privacy and Security Compliance," and authored "Managing an Information Security and Privacy Awareness and Training Program" all published by Auerbach.