European Union: Privacy and Personal Data Protection, the "Safe Harbor" Agreement

November 2002

LL File No. 2002-14028
LRA-D-PUB-000719

The Law Library of Congress, Global Legal Research Directorate
(202) 707-5080 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

LL-FLB 2002.08
2002-14028

EUROPEAN UNION: PRIVACY AND PERSONAL DATA PROTECTION, THE "SAFE HARBOR" AGREEMENT

TABLE OF CONTENTS

FOREIGN LAW BRIEFS are informative and analytical papers that address current and often controversial foreign legal and/or legislative issues, or developments in international law. They are produced by the Directorate of Legal Research of the Law Library of Congress. The Directorate staff consists of foreign legal specialists– who are foreign-trained lawyers from over 20 jurisdictions– and its multilingual legal research analysts.

For further information about the topic of this Foreign Law Brief, the author may be reached through the Director of Legal Research at (202) 707-9148. For foreign and comparative law research generally, please call the Directorate's Inquiry Line at: (202) 707-4351.

LL-FLB-2002-08
2002-14028

LAW LIBRARY OF CONGRESS

FOREIGN LAW BRIEF

EUROPEAN UNION:

PRIVACY AND PERSONAL DATA PROTECTION, THE "SAFE HARBOR" AGREEMENT

Since the mid-1990s, the European Union has introduced three directives designed to protect the "fundamental freedoms and rights of natural persons and in particular their right to privacy." The first, introduced in October 1995, became effective in 1998. It lays down the general principles on data protection and aims to safeguard the right to privacy with respect to the processing of personal data. The second was adopted in 1997, and repealed in 2002, focused specifically on the processing of personal data and the protection of privacy in the telecommunications sector. The third Directive on Privacy and Electronic Communications was adopted in July 2002, and adapts the repealed 1997 Directive to technological advances in electronic communications services.

This brief analyzes the critical provisions of the 1995 Data Protection Directive that became quite controversial because of their significant implications on the transfer of personal data by businesses to any non-EU country. Member States of the European Union in transposing the Directive into national law are required to ensure that personal data is transferred only to third countries which meet the "adequacy" standard. After long negotiations, the EU and the U.S. Department of Commerce reached an accord, the so-called "Safe Harbor" Agreement. It includes the Privacy Principles and related Frequently Asked Questions under which transfer of data from the EU to the United States is possible only by those companies which comply with these principles. The brief then analyzes the provisions of the 2002 Directive.

I. Background and Analysis

The right to privacy is a recognized fundamental human right enshrined in a number of international legal instruments. Article 12 of the Universal Declaration of Rights and article 17 of the International Covenant on Civil and Political Rights safeguard the right to privacy. Article 8 of the European Convention of Human Rights and Fundamental Freedoms also contains the right to privacy. In 1981, the Council of Europe adopted Convention No. 108 on the Protection of Individuals with Regard to Automatic Processing of Personal Data. Moreover, the United Nations and the Organization for Economic Cooperation and Development (OECD) have adopted guidelines addressing the issue of protecting the privacy and trans-border flow of personal data.

Even though the origins of the right to privacy may be traced in the United States to the 19th century, currently the United States follows a sectoral approach on this issue which encompasses legislation, regulation, and self-regulation for the private sector. By comparison, the European Union, based on the view that the right to privacy is a basic human right, deals with the issue of privacy in a radically different manner. The EU has adopted a comprehensive legal framework to protect the personal

data of individuals. The Treaty on the European Union provided the legal justification for such an action by explicitly stating that "the Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms" as such rights "result from the constitutional traditions common to the Member States, as general principles of Community law." The right to protection of one's personal data is also enshrined in the Charter of the EU. Other reasons that led the European Commission to take legislative action were the disparities in data protection laws that have existed since the 1970s in the Member States of the European Union, and the establishment of an open market where personal data would be able to flow without obstacles within the Community. Another equally strong reason was the development of electronic commerce as well as the tremendous increase of cross-border data flow due to the progress made in communication technology.

The 1995 adoption of Directive No. 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, hereafter the Data Protection Directive, became the topic of an intense debate between the European Union and the United States. As of its implementation date of October 25, 1998, any transfer of data to a third country which did not meet the adequacy criterion as established in article 26 of the Data Protection Directive, could be prohibited. This specific provision, due to its potentially adverse effects on U.S. businesses that engage in data collection and transfer, as a possible trade barrier, caused the beginning of a dialogue between the U.S. Department of Commerce and the European Commission.

On July 27, 2000, after protracted negotiations, the European Commission finally gave its approval to the "Safe Harbor" Agreement. The endorsement was in the form of a decision issued pursuant to the Data Protection Directive on the adequacy of the protection provided by the Safe Harbor Principles and related Frequently Asked Questions issued by the U.S. Department of Commerce. This decision, which binds the 15 Members of the European Union and was adopted in spite of the European Parliament's previous reservations as to whether the agreement satisfied the adequacy criterion, eliminates a potential trade barrier between the European Union and the United States.

The two documents, consisting of the Safe Harbor Principles and the related Frequently Asked Questions, reconcile the opposing views on privacy and personal data protection held by the European Union and the United States. Pursuant to the Principles, in order to avert any penalties, a U.S. company or organization that receives personal data from any EU Member must voluntarily declare its commitment to the Safe Harbor Principles. Based on these Principles, a presumption is created to the effect that companies which adhere to these Principles and are included in the list kept by the Department of Commerce, meet the adequacy standard required by the Directive. Complaints of infringements on the Principles will be investigated by the appropriate government bodies, either the Federal Trade Commission or the U.S. Department of Transportation.

In brief, U.S. organizations that voluntarily commit to the Safe Harbor Principles must adhere to the following requirements:

- **Notice.** Individuals must be informed about the purposes and uses of data about them and whether such data will be transferred to third persons.
- **Choice.** Individuals must be given a choice to decide whether or not their personal data can be disclosed to a third party or used for purposes other than those for which they were initially collected.
- **Onward transfer.** Organizations that transfer data to a third party, must first comply with the first

two requirements. Moreover, the organization must ensure that the third party adheres to the Principles or that it meets the adequacy criterion. In this case, the organization does not bear liability if the third party uses the data in a manner incompatible with the Directive.

- **Security.** Organizations must take reasonable precautionary measures to safeguard personal data from loss, destruction, unauthorized access, and disclosure.
- **Integrity.** Personal data must be used only for the intended purposes for which they were collected.
- **Access.** Individuals must be granted the right to access their personal data and be able to amend, correct, or delete the information about them.
- **Enforcement.** Organizations must provide individuals with recourse mechanisms if their rights have been violated and also penalties for the organization itself if it infringes upon the Principles.

A. Analysis of Directive No. 95/46/EC on Personal Data Protection

The preambular provisions of the Data Protection Directive specify the principal reasons for its adoption: "data-processing systems are designed to serve man and must respect the fundamental rights and freedoms of individuals, notably the right to privacy." The Data Protection Directive, which used as a model the Council of Europe Convention No. 108 (1981) and the OECD (1980) and 1990 UN guidelines, aims to harmonize the domestic provisions of the Member States on data protection by balancing two fundamental but competing principles: to safeguard the right to privacy through comprehensive regulation of the processing of personal data of individuals and at the same time to ensure the uninterrupted flow of such data within the Community. It also aims to ensure that the transfer of personal data to countries outside the European Union is possible only when such third countries provide "adequate" standards of protection.

A key requirement of the Data Protection Directive is that data processing must meet certain principles to ensure protection. In order to meet this requirement, the Directive imposes a number of obligations, such as quality control and technical security, on persons, public authorities, enterprises, agencies, and other bodies responsible for processing. It also confers on the person involved in the data (data subject) certain important rights in order to safeguard his/her right to privacy.

1. Scope

The scope of the Directive is broad. In general, it covers all processing of personal data in the public and private sector. Personal data are defined as "any information relating to an identified or identifiable natural person," that is, the data subject. Processing is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means." Consequently, the Directive applies to data processed through automatic means as well as to data which are part of, or intended to be part of, a non-automated "filing system," *i.e.*, manual processing. An indicative list of processing activities includes collection, organization, storage, retrieval, disclosure by transmission, and erasure.

A number of activities associated with the processing of personal data fall outside the scope of the Directive: processing related to public security, defense, State security, criminal law; and activities related to areas falling within the domain of the Member States; and processing undertaken by a natural person

as a clearly personal or household activity, such as the preparation of an address book, personal correspondence, and others.

2. Requirements of Lawful Processing

As a general rule, personal data may be processed in the following enumerated cases:

- the data subject has granted consent
- processing is essential for the performance of a contract in which the data subject is a party
- processing is essential for compliance with a legal obligation to which the controller is a subject
- in order to protect significant interests of the data subject
- in order to perform a task in the exercise of official authority vested in the controller, or a task done for the public interest
- for lawful interests pursued by the controller or by a third party, unless the data subject's right over personal data overrules such interests

3. Sensitive Data

Sensitive data, that is data related to racial or ethnic origin, religious or philosophical beliefs, political opinions, memberships in trade unions as well as data pertaining to one's health or sex life, are treated in a strict manner. Under the Directive, Member States are obliged to prohibit the processing of such data. A number of exceptions do apply. Processing is allowed in the following cases:

- if the data subject consents, Member States are free to provide otherwise
- in order to carry out the obligations of the controller in the area of employment law (Member States must authorize such processing.)
- in order to protect important rights of the data subject, or if the data subject is legally or physically incapacitated to give his/her consent
- if it is done by a foundation, association, or other non-profit organization under certain conditions
- if the data subject has made such data public
- if there are substantial safeguards, then additional exemptions may be established based on national law or supervisory authority
- if the processed data is related to offenses, criminal convictions, or security measures and done only by an official authority and under certain safeguards (The processing of data related to administrative sanctions or judgments in civil offenses under the control of an official authority is left to the discretion of Member States.)

4. Medical Data

In general, since medical data are also considered sensitive data, they fall also under the general prohibition rule. However, processing of medical data is permitted, provided that the data subject has granted consent and under the following circumstances: a) it takes place for preventive purposes, for

medical diagnosis, or for the provision of care, treatment, or the management of health care services; and the data are processed by a health professional under national law or rules established by a national competent body to the obligation of professional secrecy.

5. Processing of Data and Free Expression

The Directive allows Member States to claim exemption from restrictions on processing personal data done only for journalistic, artistic, or literary purposes. However, exemptions are allowed only and if they are necessary in order to reconcile the right to privacy with freedom of expression.

6. Responsibilities of Controllers

The controller, that is the person or body "which determines the purposes and the means of processing," must ensure that processing personal data takes place under the principles of security and confidentiality. Thus, the controller must take certain measures, either technical or organizational, to protect the data from accidental or unlawful destruction or accidental loss, alteration, or unauthorized disclosure. The measures must be appropriate to the risks inherent in the processing and the nature of the data to be protected. The controller must also ensure that he/she adheres to a number of additional standards, including the data being:

- processed fairly and lawfully
- collected for a specific, explicit, and legitimate purpose
- adequate, relevant, and not excessive
- accurate and up-to-date, as necessary
- kept only as long as necessary

When the processing of data takes place under the control of a processor, the Directive requires that the following additional conditions be met:

- the processor be chosen by the controller
- their relationship be regulated by a written contract
- the processor shall act only on instructions given from the controller
- the processor must implement the same technical or organizational safeguards as the controller

The controller or his/her representative must notify the supervisory authority responsible for monitoring implementation of the Directive.

7. Rights of the Data Subject

Data subjects have the following rights under the Directive: right of information, right of access, and right to object.

a) Right of Information

If the data were collected from the data subject, the latter is entitled to know the identity of the

controller or his/her representative, the purpose of processing the data, and any other information related to recipients of data, including whether or not responses to data are voluntary and the existence of the right of access and the right to correct the data.

If the data have not been obtained from the data subject, the latter has the same rights as above.

b) Right of Access

The right of access involves the following elements that the data subject is entitled to:

- confirmation without undue delay whether or not any processing of personal data occurs, the purpose of processing, groups of data, and recipients of such data
- communication of the data being processed and their source and of the logic involved in automatic processing
- opportunity to remedy the processing of data or erase or block the processing in the case of incomplete or inaccurate data or if, in general, it infringes upon the standards of this Directive
- notification to third parties of any rectification, elimination, or blocking that has occurred in the processing of personal data

c) Right to Object

The data subject has the right to object to the processing of personal data related to him/her if the data are being processed for marketing purposes or to be informed and use his/her right to object prior to initial disclosure of the data to a third person. A data subject has also the right to object when processing is necessary for a task for the public interest and for the legitimate interests of the controller.

8. Transfer of Personal Data

The critical provisions of the Directive related to the transfer of personal data to third countries are included in articles 25 and 26. The general rule is that transfer of personal data to a third country, that is any non-EU country, is permitted only if that country "ensures an adequate level of protection." Such restrictions on the trans-border data flow are in line with GATS (art. XIV), under which the blocking of personal data flows is permissible.

The Working Party on Protection of Individuals with regard to the processing of personal data established under the Directive has issued guidelines on making an assessment. Thus, assessment criteria of the "adequacy" level include the nature of data, purpose and duration of the processing, country of origin and country of final destination, general and sectoral legal rules in force, as well as professional rules and security measures in the third country.

When a third country does not meet the criterion, each Member State must prevent the transfer of data to the said country while simultaneously informing the other Members and the Commission of this finding. Transfers of data are allowed in third countries which do not satisfy the adequacy requirement if one of the following conditions is met:

- The data subject has given his/her consent to the transfer.
- The transfer is necessary for the performance of a contract between the data subject and the

controller, or for the performance of a contract between the controller and a third party for the interest of the data subject.

- The transfer is necessary in order to protect significant interests of the data subject.
- The transfer occurs for important public interest reasons.
- The transfer is made from a register intended to give information to the public.

Moreover, Member States have the discretion to authorize the transfer of data to a third country, even though that country does not meet the "adequacy" standard, if the controller deems that the third country provides sufficient safeguards with respect to the fundamental rights and freedoms and especially with the right to privacy. This could take place through a contract between the exporter and importer of the data.

In 2001, the Commission established standard contractual clauses to facilitate the trans-border flow of data. The clauses allow third businesses or organizations operating in third countries to transfer data provided that they adopt the clauses in their contracts. U.S. organizations or companies that have joined the Safe Harbor do not need to adhere to such clauses; however, other companies, outside of this system, must do so.

9. Enforcement

In order to accomplish its goal of providing effective protection of the right to privacy, the Directive provides mechanisms to ensure compliance with the principles of the Directive, at the national and Community level. It also requires Member States to provide recourse for individual citizens whose personal data have been violated as well as to impose sanctions for those who infringe on the provisions of the Directive.

At the national level, each Member State is obliged to establish one or more public authorities responsible for monitoring the application of the Directive. The authorities are empowered with investigative power, the power to intervene, and the power to institute legal proceedings.

At the Community level, the Directive established a Working Party on the Protection of Individuals with regard to the Processing of Personal Data. The"Working Party" has advisory status and is composed of representatives of the supervisory authorities established by Member States, a representative chosen by the Commission, and a representative of the authority established for the EU institutions. Among the powers conferred on the Working Party is the power to advise the Commission on proposed amendments of the Directive. It is also obliged to prepare and forward to the Commission, the Parliament, and the Council an annual report on the status of implementation of the processing of personal data in the Community and third countries. Thus, on June 25, 1997, the Working Party prepared its first report on the measures taken by the Member States in transposing the Directive into internal law. Another report followed in 1998 on the changes that took place in the interim period.

A committee, composed of the representatives of the Member States and chaired by one chosen by the Commission, has been established to assist the Commission and express its opinion on draft measures prepared by the Commission.

10. Liability and Judicial Remedies

Member States are responsible under the Directive to provide every person with the right to a judicial remedy in case of the breach of rights arising from the processing of personal data. They also must ensure that a person who has suffered damage due to unlawful processing receive compensation from the controller. It is the responsibility of the controller to prove that he/she is not responsible for events giving rise to the damage. Moreover, Member States must impose sanctions in case the provisions of the Directive are violated.

B. Directive No. 2002/58/EC on Privacy and Electronic Communications

The increased use of digital technologies in public telecommunications networks and specifically the introduction of Integrated Service Digital Network (ISDN), as well as the need to protect the privacy of the users led to the adoption in 1997 of Directive No. 66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. That Directive basically applied the principles and standards embodied in the 1995 Directive to the telecommunications sector.

Directive No. 97/66/EC was repealed in 2002 by Directive No. 58/EC. The new Directive harmonizes the provisions of the repealed Directive to new and future developments in the electronic communications sector. Similar to the old Directive, the new one complements Directive No. 95/46/EC in regard to the rules on the protection of the fundamental rights and freedoms with respect to the processing of personal data in the electronic communications sector. Its scope is broader than that of Directive No. 95/46, as it also affords protection to the legitimate interests of subscribers of electronic communications who are legal entities. Acceptable forms of consent are broad and include the checking of a box in a particular website. The Working Party on the Protection of Individuals concerning the Processing of Personal Data, as founded by Directive No. 95/46/EC, is also responsible for matters that fall within the scope of Directive No. 2002/58/EC. The new Directive must be implemented by the Member States by October 31, 2003.

1. Highlights of the New Directive

New and expanded definitions are provided by this Directive:

- **User.** any natural person who uses a publicly available electronic communications service, either for private or business purposes, without being necessarily a subscriber to this service
- **Traffic data.** any data processed in order to convey a communication on an electronic communications network or for billing purposes
- **Location data.** any data processed through an electronic communications network that indicates the location of the terminal equipment of a user
- **Communication.** any information exchanged conveyed between parties through a publicly available electronic communications service
- **Call.** a connection established through a publicly available telephone service which allows two-way communication in real time
- **Electronic mail.** any text, voice, sound, or image message communicated through a public communications network which can be stored in the network or in the recipient's terminal

equipment until it is received by the recipient

- **Value added service.** any service which requires the processing of traffic data or location data beyond what is necessary for the transmission of a communication or billing thereof; may include advice on the least expensive tariff packages, traffic information, road guidance, tourist information and weather forecasts (Recital 18 of Preamble)

2. Confidentiality of Communications

The Directive guarantees the confidentiality of communications and traffic data. Consequently, it requires that Member States adopt domestic legislation to implement the principle of confidentiality. In particular, Members are required to prohibit the following actions:

> Listening, taping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except in specified cases provided under article 15, paragraph 1.

The above prohibition does not apply to any legally permitted recording of communications and traffic data when such recording takes place during lawful business for evidentiary purposes. Parties involved should be informed, prior to the recording, about the recorded communication, its purpose, and duration of storage. Recital 23 states that such a communication must be erased as soon as possible and at the latest "by the end of the period during which the transactions can be lawfully challenged."

Additionally, Member States are required to ensure that the use of an electronic communications network to store information or to gain access to information stored in the terminal equipment of a subscriber is permitted only when the following two conditions are met: 1) the subject (subscriber or user) is informed about such use, in accordance to the principles of Directive No. 95/46/EC; and 2) the subject has been given the right to refuse such processing.

3. Traffic Data

In comparison to the repealed Directive, the 2002 Directive defines traffic data broadly to include not only data generated through traditional telephone calls but also data generated through the transmission of communications over the Internet. The Directive establishes rules concerning the processing of traffic data and specifies the persons who are legally authorized to do so.

a) Processing Traffic Data

In general, the Directive requires that traffic data on subscribers and users which have been processed and stored by the provider of a public communications network or an electronic communications service be erased or made anonymous when they are no longer needed. The following exceptions apply:

- Traffic data which are essential for billing purposes and interconnection payments may be processed for a limited period, that is, until the end of the period during which the bill can be challenged or payment pursued. The service provider is obliged to inform the subscriber or the user of the kinds of traffic data that are processed and of the duration of such processing.

- Traffic data used for marketing purposes or for the provision of value added services may be

processed only to the extent and duration necessary for such services provided that the subscriber or user has consented to such processing and has been given the option to withdraw his/her consent at any time. In this case, the service provider is obliged to inform the subscriber prior to obtaining his/her permission.

b) Persons Authorized to Process Traffic Data

Only persons who act under the authority of the providers of public communications networks and publicly available electronic communication services that deal with billing or traffic management, customer inquiries, fraud services, or providing a value added service, are permitted to process traffic data and only to the extent that is necessary in order to perform the above mentioned tasks.

4. Itemized Billing

Under the Directive, subscribers have the option to receive non-itemized bills. The Directive allows Members to regulate the issue of reconciling the right to privacy of callers with the right of subscribers who receive itemized bills. The Directive brings as a possible example the use of privacy enhancing methods of communications or payments.

5. Presentation and Restriction of Calling- and Connected- Line Identification

If calling-line identification is offered, Member States are required to give the calling subscriber the option to eliminate calling-line identification, without charge, on a per-call/per-line basis. This also applies to calls originating in the Community that are made to third countries.

At the same time, the called subscriber must also have the equivalent option to prevent the calling-line identification of incoming calls without charge. He/she must also have the option to reject incoming calls when the calling line has been eliminated by the calling user. When presentation of connected-line identification is offered, the called subscriber must be able to eliminate the connected line. These provisions apply to calls made to the Member States that originate in third countries.

6. Location Data Other than Traffic Data

This is a new subject not previously covered by the repealed Directive. Article 6 introduces protection for subscribers and users with regard to mobile location information services. Recital 14 of the Preamble clarifies that location data may refer to "the latitude, longitude and altitude of the user's terminal equipment, to the direction of the travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located."

The Directive establishes the instances under which processing of location data concerning users or subscribers can occur and the authorized persons to do so. Thus, processing may occur under the following conditions:

- are made anonymous
- users or subscribers have ben informed
- users or subscribers have consented to the processing only to the extent and for the duration necessary for the provision of a value added service

Users or subscribers who have consented to the processing of location data must have the option to temporarily refuse the processing of such data through the use of simple means. No additional fee may be imposed for such feature.

Persons authorized to process location data are those who act under the authority provided by the public communications network or publicly available communications service of the third party that provides the value added service.

7. Exemptions

Elimination of calling-line identification can be suspended in case of malicious or nuisance calls, the Directive gives the subscriber the right to request temporarily and upon application the malicious or nuisance calls to be traced; and in case of emergency calls made to law enforcement agencies, ambulance services, and fire departments.

8. Directories of Subscribers

It is a common practice to disseminate printed or electronic directories of subscribers. Such a practice may infringe upon the privacy of individual subscribers if it occurs without providing any safeguards against possible abuse and misuse. Article 12 of the Directive aims to eliminate such abuses by granting control to subscribers as to whether and which of their personal data will be included in a directory. It specifies that subscribers must be given specific information, free of charge, and before their personal data are included in the directory on the following two aspects: a) the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory inquiry services; and b) any additional usage possibilities based on search functions inserted in electronic versions of the directory, such as reverse search capability which allows users of the directory to find out the name and address of the subscriber based solely on his/her telephone number.

The person who collects the data to be included in public directories also bears the responsibility to provide the subscribers with information on the purpose of the directories and whether the directory is going to be further disseminated as well as the nature of the recipients. As Recital 39 of the Preamble elaborates, any transmission of personal data "should be subject to the condition that the data may not be used for other purposes than those for which they were collected." Furthermore, if the data are going to be used for additional purposes, a new consent is necessary and should be obtained either by the party that collected the data initially or by the party to whom the data is transferred.

9. Unsolicited Communications

Article 13 on unsolicited communications prohibits the use of automatic calling machines, fax, or electronic mail for direct marketing purposes without the prior consent of subscribers. Recital 40 of the Preamble explains that the reason for imposing such a requirement is because in general, unsolicited communications impose an undue burden and/or cost on the recipient and the volume of such may cause problems to electronic networks and terminal equipment.

However, the Directive allows the use of electronic personal data for electronic mail by a natural or a legal person that obtains such data through the sale of a product or a service to be used for direct marketing of its own similar products or services under the condition that the natural or legal person has given customers the chance to object free of charge to such use of their electronic data.

Moreover, the Directive specifically prohibits another form of use of electronic mail for direct marketing. This is the case where the identity of the sender is either disguised or hidden or when a valid address is not provided.

10. General Limitations Imposed by Member States

Pursuant to the standards emanating from the case law of the European Court of Human Rights in Strasbourg, the Member States may impose certain restrictions to the right of privacy as long as such restrictions constitute a "necessary, appropriate and proportionate measure within a democratic society." Moreover, any measures adopted by Member States that curtail the right to privacy must be in conformity with article 6(1) and (2) of the Treaty of European Union as stated previously.

Reasons for imposing such restrictions include national security, defense, public safety, and the prevention, investigation, detection, and prosecution of criminal offenses. The following may be subject to restrictions:

- confidentiality of communications (art. 5)
- traffic data (art. 6), however, data retention is allowed only for a limited period
- presentation and restriction of calling- and connected- line identification (art. 8(1), (2), (3) and (4))
- location data (art. 9)

11. Judicial Remedies, Liability, and Sanctions

The same provisions of Directive No. 95/46/EC on judicial remedies, liability issues, and sanctions, as stated above, apply also to this Directive.

II. Chronology of Events

10/24/1995	Adoption of Directive No. 95/46/EC of the European Parliament and the Council on the protection of individuals in regard to the processing of personal data and on the free movement of such data
12/15/1997	Adoption of Directive No. 97/66/EC of the European Parliament and the Council on the processing of personal data and the protection of privacy in the Telecommunications Sector
7/24/1998	Working Party on the Protection of Individuals: Transfer of Personal Data to Third Countries, applying articles 25 and 26 of the EU Data Protection Directive.
10/25/1998	Both Directives come into effect
Fall 1998	Beginning of the dialogue between the European Commission and the U.S. Department of Commerce
01/26/1999	Opinion 1/99 of the Working Party concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government

06/7/1999	Opinion 4/99 complemented by the working document of July 7 1999
12/3/1999	Opinion 7/99 on the Level of Data Protection by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on November 15 and 16, 1999, by the U.S. Department of Commerce
7/27/2000	Commission Decision pursuant to Directive No. 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the U.S. Department of Commerce
11/21/2000	Working document: Privacy on the Internet– An Integrated Approach to Online Data Protection
05/17/2001	Recommendation 2/2001 on certain minimum requirements for collecting personal data online in the European Union
06/15/2001	Commission Decision on standard contractual clauses for the transfer of personal data to third countries, under Directive No. 95/46/EC
12/27/2001	Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive No. 95/46/EC
05/30/2002	Working document: Determining the International Application of EU Data Protection Law to Personal Data processing on the Internet by non-EU Based Websites
07/08/2002	Working document: Functioning of the Safe Harbor Agreement
7/12/2002	Adoption of Directive No. 2002/58/EC of the European Parliament and of the Council July 12, 2002, Directive on Privacy and Electronic Communications
10/11/2002	Opinion 5/2002 adopted on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (Sept. 11, 2002) on mandatory systematic retention of telecommunications traffic data

III. Congressional Action

The following is a selective list of bills dealing with privacy issues that were introduced in the 107th U.S. Congress:

Federal Privacy and Data Protection Policy Act of 2002 Senate (June 17, 2002), S. 2629.IS

To provide for an agency assessment, independent review, and an Inspector General report on privacy and data protection policies of Federal agencies, and for other purposes.

Stop Taking Our Health Privacy (STOHP) Act of 2002 H.R. (Oct. 16, 2002), H.R. 5646.IH

To restore standards to protect the privacy of individually identifiable health information that were weakened by the August 2002 modifications, and for other purposes.

Federal Agency Protection of Privacy Act (passed the H.R. on Oct. 2, 2002, introduced in the Senate on Oct. 10, 2002), H.R. 4561.EH, S. 2492.IS

To amend Title 5 of the United States Code to require that agencies, in promulgating rules, take into consideration the impact of such rules on the privacy of individuals, and for other purposes.

Consumer Privacy Protection Act of 2002 H.R. (May 8, 2002), H.R. 4678.IH

To protect the privacy of individuals in interstate commerce and give consumers the right to limit sale or disclosure of information.

Location Privacy Protection Act of 2001 Senate (July 11, 2001), S. 1164.IS

To provide for the enhanced protection of the privacy of location information of users of location-based services and applications, and for other purposes.

Gun Sale Anti-Fraud and Privacy Protection Act Senate (July 26, 2001), S. 1253.IS, H.R. 2778.IH

To protect the ability of law enforcement personnel to effectively investigate and prosecute illegal gun sales and protect the privacy of the American people.

Personal Information Privacy Act of 2001 H.R. (Apr. 4, 2001), H.R. 1478.IH

To protect the privacy of individuals concerning their social security number and other personal information, and for other purposes.

Social Security Number Privacy Act of 2001 Senate (Feb. 14, 2001), S. 324.IS

To amend the Gramm-Leach-Bliley Act, to prohibit the sale and purchase of the social security number of an individual by financial institutions, to include social security numbers in the definition of nonpublic personal information, and for other purposes.

Consumer's Right to Financial Privacy Act H.R. (Aug. 2, 2001), H.R. 2720.IH

To protect the privacy of consumer information.

Online Privacy Protection Act of 2001 H.R. (Jan. 3, 2001), H.R. 89.IH

To require the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected from and about individuals who are not covered by the Children's Online Privacy Protection Act of 1998 on the Internet, to provide greater individual control over the collection and use of that information, and for other purposes.

Financial Information Privacy Protection Act of 2001 Senate (Jan. 22, 2001), S. 30.IS

To restrict the transfer of information about personal spending habits, restrict the use of health information in making credit and other financial decisions and to give consumer the right to access and correct information.

IV. Conclusion

Adoption by the European Union of the two Directives addressing privacy issues in relation to personal data reflects its commitment to protect the citizens of the Member States against abuse of their privacy right. The significance and repercusssions of these two legislative measures become even more dramatic in the current information age in which the tremendous growth of electronic commerce has dramatically facilitated the dissemination, storage and use of personal data. Considerable controversy arose over the extraterritorial reach of the 1995 Directive since it directly affects the manner by which businesses and organizations in third countries handle and process personal data. The expansion of the EU with the accession of 10 additional countries may render the transfer of personal data even more problematic. The United States and the European Union have reached a compromised solution by establishing the Safe Harbor agreement, which is currently under evaluation by a Working Party. In some cases, in order to qualify for lawful transfer of data, organizations or businesses located in third countries may choose to follow the model contracts adopted by the Commission

The transposition of the 1995 Directive into national laws has proved to be cumbersome. A number of Member States adopted domestic legislation by the 1998 implemetation deadline. Luxembourg in particular adopted national legislation just recently, and France and Ireland have not yet completed the legislative process. Moreover, a number of divergencies have surfaced among those Member States that implemented the provisions of the Directive. These implementation difficulties and other critical issues were carefully examined and thoroughly discussed in a conference on Data Protection organized by the Commission from September 30 to October 1, 2002, in preparation for the Commission's forthcoming evaluation report of the 1995 Directive. Some of the issues discussed were developments in the information society; Internet and privacy enhancing technologies; the processing of sound and image data; and international issues, such as international data transfers, applicable law, and jurisdiction.

V. Selected Bibliography

Monographs

A Business Guide to Changes in European Data Protection Legislation, Cullen International, 1999.

On-line Services and Data Protection and Privacy, vol. II, European Commission, Directorate-General Internal Market and Financial Services, 1998.

P. Swire and R. Litan, *None of Your Business,* Washington, DC.

Articles

Barbara Crutchfield George et al., "U.S. Multinational Employers: Navigating through the 'Safe Harbor' Principles to Comply with the EU Data Privacy Directive," 38 American Business Law Journal, 735 (Summer 2001).

D. R. Tan, "Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union," 21 Loy.L. A. Intl. and Co. L.J., 661 (1999).

David A. Castor, "Treading Water in the Data Privacy Age: An Analysis of the Safe Harbor's First Year," 12 Indiana International and Comparative Law Review, No. 2265 (2002).

F. H. Gate, "Business Law Symposium: Entering a New Era in Telecommunications Law: Privacy and Telecommunications," 33 Wake Forest L. Rev. 1 (1998).

G. Shaffer, "The Power of EU Collective Action: the Impact of EU Data Privacy Regulation on U.S. Business Practice," 5 Eur. L.J., No. 4, 419-437 (1999).

Mike Ewing, "The Perfect Storm: the Safe Harbor and the Directive on Data Protection," 24 Houston Journal of International Law 315 (Winter 2002).

Prepared by Theresa Papademetriou
Senior Legal Specialist
Directorate of Legal Research
Law Library of Congress
November 2002