1 OKLA. J. L. & TECH. 11 (2004)
www.okjolt.org

Abstract

Dr. Alexander Zinser, LL.M., is a Senior Attorney at Agilent Technologies International, Sarl, Morges, Switerland, a subsidiary of Agilent Technologies Inc., Palo Alto, California. Below, Dr. Zinser provides an overview of the European Data Protection Directive ("Directive"), with particular emphasis on international data transfers of personal information between the European Union and the United States. Part I provides a comparative look into the different approaches to data protection taken by the United States and the European Union. Part II and III, respectively, discuss Safe Harbor Principles available to U.S. companies that voluntarily choose to adhere to certain data protection guidelines and the legal basis for the Safe Harbor arrangement derived from the Directive. Part IV offers a comprehensible breakdown of each Safe Harbor Principle as well as ancillary provisions regarding dispute resolution and enforcement of the Principles. Lastly, Part V defines the powers of the European states and authorities with regard to violations of the Principles.

THE SAFE HARBOR SOLUTION: IS IT AN EFFECTIVE MECHANISM FOR INTERNATIONAL DATA TRANSFERS BETWEEN THE UNITED STATES AND THE EUROPEAN UNION?

Dr. Alexander Zinser[*]

I. Introduction

The European Union enacted the European Data Protection Directive 95/46/EC ("Directive") in 1998, which set out to protect individuals "with regard to the processing of personal data" and to promote "the free movement of such data."[1] The Directive addresses "the progress made in information technology" and how technology "is making the processing and exchange of such data considerably easier."[2] More specifically, the Directive will "lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States."[3] The Di-

[*] Dr. jur.; LL.M.; Senior Attorney at Agilent Technologies International, Sarl, Morges, Switzerland, a subsidiary of Agilent Technologies Inc., Palo Alto, California. The views expressed in this article are the author's own and do not necessarily reflect those of Agilent Technologies.

[1] Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter Directive] (promulgated by the European Parliament and the Council of the European Union). Personal data is "any information relating to an identified or identifable natural person;…an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." *Id.* art. 2(a). Processing of such data "mean[s] any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection,…use, disclosure by transmission, dissemination, erasure or destruction." *Id.* art. 2(b).

[2] *Id.* § 4.

[3] *Id.* § 5.

rective ensures the movement of personal data without restrictions within the European Union: Member States are no longer allowed to restrict the freedom of transferring personal data by arguing that another Member State has not implemented procedures ensuring an adequate level of data protection.[4] The Directive also regulates the transfer of data outside the boundaries of the European Union and overseas. According to Article 25 of the Directive, such a transfer is allowable only if an adequate level of data protection is secured in the recipient country.[5] With regard to data transfers from the European Union to the United States, data controllers in the United States are required to ensure an adequate level of protection in order to be in compliance with European data protection laws. However, the fulfillment of the requirement of adequacy is problematic.

II. The U.S. and E.U. Approach to Data Protection

The approach to data protection by the United States and the European Union are completely different. Basically, the U.S. approach relies on a mix of self-regulation and legislation, whereas the European Union has adopted an all-encompassing legislative approach.[6] The European "approach toward data protection is grounded in the concept of privacy as a fundamental human right."[7] Essentially, the E.U. presumes that "a just and free society results only when individuals are able to interact with self-determination and dignity."[8] However, in the U.S., the states tend to intercede "between organizations and individuals to create parity," and guarantees this fundamental right to data protection by means of preventative

---

[4] David I. Bainbridge, *Processing Personal Data and the Data Protection Directive*, 6 INFO. & COMM. TECH. L. 17, 18 (1997).
[5] Directive, *supra* note 1, art. 25.
[6] Quentin Bargate & Martin Shah, *The E.U./U.S. Safe Harbour Data Protection Agreement-A Shotgun Marriage?*, 15 J. I. B. L. 177 (2000).
[7] William J. Long & Marc Pang Quek, *Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise*, JOURNAL OF EUROPEAN PUBLIC POLICY 325, 331 (2002), *available at* http://dandini.ingentaselect.com/vl=7015360/cl=148/nw=1/fm=docpdf/rpsv/cw/routledg/13501763/v9n3/s1/p325 (last visited Mar. 6, 2004).
[8] *Id.*

legislation.[9] The Americans are more fearful of the invasion of data protection and privacy from the states rather than from the market.[10] In fact, the United States legal system treats data protection and privacy as a personal property right that may be ignored.[11]

A comparative look into both systems reveals that "the European approach is more proactive," whereas "American policy-making is more reactive" and will step in to tailor specific regulatory solutions only where problems arise.[12] An important element of the United States data protection regime is self-regulation. The industry believes that the bureaucracy is not flexible enough and unable to cope with the changes and innovative power of the economy.[13] In sum, Americans and Europeans have fundamental differing views with regard to the necessary legal protection to be afforded to their respective citizens. Therefore, each has developed different data protection regimes: the European Union established comprehensive data protection legislation, and regards privacy as a fundamental right to be protected proactively by the government, but the United States legislation is primarily based "on industrial self-regulation with some protection through the courts."[14] The American view derives from the belief that data protection is a qualified right and any governmental intrusion is undesirable.[15] Further, the data protection regime in the United States is fragmented and narrowly targeted to cover specific "sectors and concerns."[16] This cultural difference raised several problems with regard to the Safe Harbor negotiations.

---

[9] *Id.*
[10] *Id.*
[11] *Id.* at 331-32.
[12] *Id.* at 332.
[13] *Id.*
[14] *Id.* at 333.
[15] *See id.* at 332.
[16] Gregory Shaffer, *The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice,* 5 EUR. L.J. 419, 423 (1999), *available at* http://www.blackwell-synergy.com/servlet/useragent?func=synergy&synergyAction=showTOC&journalCode=eulj&volume=5&issue=4&year=1999&part=null (last visited Mar. 6, 2004).

III. Safe Harbor Negotiations

The implementation of the Directive "has precipitated a clash between the differing information cultures"[17] and data protection regimes. In the opinion of the Europeans, "the United States has disappointingly weak protection of individual rights to privacy."[18] In contrast, the American view perceives "the Directive's regulations" as causing very "costly compliance measures when there is little or no social harm caused by unregulated practices."[19] Though it is clear to European officials that the United States will not pass comprehensive data protection laws, the Europeans still exhibit a willingness to find workable solutions.[20] Otherwise, it would be difficult to carry out data transfers between the United States and the European Union "after the effective date of the Directive."[21]

The United States Department of Commerce, on behalf of the U.S. Government and Directorate General XV of the European Commission, began negotiations on how to fulfill the adequacy requirement[22] of the Directive. Both parties discussed the creation of a so-called Safe Harbor for United States companies who voluntarily choose to adhere to certain data protection principles. There would be a presumption of adequacy for those companies within the Safe Harbor Principles so that a data transfer from the European Union would be in line with the Directive.[23] In November, 1998, Ambassador David L. Aaron, Undersecretary for International Trade of the United States Department of Commerce, wrote a letter to

---

[17] PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE AND THE EUROPEAN PRIVACY DIRECTIVE 153 (1998) (Brookings Institution Press), *available at* http://brookings.nap.edu/books/081578239X/gifmid/153.gif (last visited Mar. 6, 2004).
[18] *Id.*
[19] *Id.* at 154, *available at* http://brookings.nap.edu/books/081578239X/gifmid/154.gif (last visited Mar. 6, 2004).
[20] *Id.* at 173, *available at* http://brookings.nap.edu/books/081578239X/gifmid/173.gif (last visited Mar. 6, 2004).
[21] *Id.* The Directive became effective in October 1995.
[22] *See supra* Part I.
[23] Shaffer, *supra* note 16, at 428.

industry representatives asking them for comments on the draft Safe Harbor Principles.[24] In this context, it must be said that most U.S. businesses were not in favour of the European Union demands, and thus strenuously objected to them. They spent a lot of money on lobbying as they reasoned that a new data protection regime would raise significant business costs.[25]

The Working Party on the Protection of Individuals must be involved before the European Commission adopts a decision on the adequacy requirement; the Working Party has "advisory status and acts independently."[26] It was designed to "examine any questions covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures."[27] The Working Party "give[s] the Commission an opinion on the level of protection in the Community and in third countries."[28] It has delivered opinions on the level of protection provided by the Safe Harbor Principles: Opinion 1/99 on January 26, 1999;[29] Opinion 2/99 on May 3, 1999;[30] Opinion 4/99 on June 7, 1999;[31] Opinion 7/99 on December 3, 1999;[32] Opinion 3/2000 on March 16, 2000[33] and, fi-

---

[24] Letter from David L. Aaron, Undersecretary for International Trade of United States Department of Commerce, to Industry Representatives (Nov. 4, 1998), *available at* http://www.ita.doc.gov/td/ecom/aaron114.html (last visited Mar. 6, 2004).
[25] Shaffer, *supra* note 16, at 430.
[26] Directive, *supra* note 1, art. 29(1).
[27] *Id.* art. 30(1)(a).
[28] *Id.* art. 30(1)(b).
[29] Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, Opinion 1/99 (Jan. 26, 1999) ("concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States"), *available at* http://europa.eu.int/comm/internal_market/privacy/workingroup/wp1999/wpdocs99_en.htm (last visited Mar. 3, 2004).
[30] Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, Opinion 2/99 (May 3, 1999) ("on the Adequacy of the 'International Safe Harbor Principles' issued by the US Department of Commerce on 19th April 1999"), *available at* http://europa.eu.int/comm/internal_market/privacy/workingroup/wp1999/wpdocs99_en.htm (last visited Mar. 6, 2004).
[31] Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, Opinion 4/99 (June 7, 1999) (on "Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed 'Safe Harbor Principles'" and on the adequacy of the International Safe Harbor Principles, *available at* http://europa.eu.int/comm/internal_market/privacy/workingroup/wp1999/wpdocs99_en.htm (last visited Mar. 6, 2004).

nally, Opinion 4/2000 on May 16, 2000.[34] Basically, the above-mentioned Opinions cover the relevant draft of the Safe Harbor Principles including several drafts of the Frequently Asked Questions.

The United States Department of Commerce issued draft Safe Harbor Principles on November 4, 1998;[35] April 19, 1999;[36] November 15, 1999;[37] March 17, 2000;[38] June 9, 2000,[39] and the final version on July 21, 2000.[40] The drafts of Frequently Asked Questions were issued on April 19, 1999,[41] April 30, 1999,[42] November 15, 1999,[43] March 17, 2000,[44]

---

[32] Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, Opinion 7/99 (Dec. 3, 1999) ("[o]n the Level of Data Protection provided by the 'Safe Harbor' Principles as published together with the Frequently asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce"), *available at* http://europa.eu.int/comm/internal_market/privacy/workingroup/wp1999/wpdocs99_en.htm (last visited Mar. 6, 2004).

[33] Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, Opinion 3/2000 (Mar. 16, 2000) ("[o]n the EU/US dialogue concerning the 'Safe [H]arbor' arrangement"), *available at* http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2000/wpdocs00_en.htm (last visited Mar. 6, 2004).

[34] Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, Opinion 4/2000 (May 16, 2000) ("on the level of protection provided by the 'Safe Harbor Principles'"), *available at* http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2000/wpdocs00_en.htm (last visited Mar. 6, 2004).

[35] *See supra* note 24.

[36] *Draft: International Safe Harbor Privacy Principles*, U.S. Dept. of Commerce (Apr. 19, 1999), *available at* http://www.ita.doc.gov/td/ecom/shprin.html (last visited Mar. 6, 2004).

[37] *Draft: International Safe Harbor Privacy Principles Issued By the U.S. Department of Commerce*, U.S. Dept. of Commerce (Nov. 15, 1999), *available at* http://www.export.gov/safeharbor/Principles1199.html (last visited Mar. 6, 2004).

[38] *Draft: International Safe Harbor Privacy Principles Issued By the U.S. Department of Commerce*, U.S. Dept. of Commerce (Mar. 17, 2000), *available at* http://www.export.gov/safeharbor/RedlinedPrinciples31600.htm (last visited Mar. 6, 2004).

[39] *Draft: International Safe Harbor Privacy Principles Issued By the U.S. Department of Commerce*, U.S. Dept. of Commerce (June 9, 2000), *available at* http://www.export.gov/safeharbor/USPrinciplesJune2000.htm (last visited Mar. 6, 2004).

[40] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July 24, 2000), *relevant portion available at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm (last visited Mar. 6, 2004).

[41] *Draft: Frequently Asked Questions (FAQs)*, U.S. Dept. of Commerce (April 19, 1999), *available at* http://www.ita.doc.gov/td/ecom/access.html (last visited Mar. 6, 2004).

[42] Letter from David L. Aaron, Undersecretary for International Trade of United States Department of Commerce, to Colleagues (Apr. 30, 1999), *available at* http://www.export.gov/safeharbor/aaron430.htm (last visited Mar. 6, 2004).

[43] *FAQ's*, U.S. Dept. of Commerce, *available at* http://www.export.gov/safeharbor/sh_historicaldocuments.html (last visited Mar. 6, 2004) (under the heading "Week of November 15, 1999").

[44] *FAQ's*, U.S. Dept. of Commerce, *available at* http://www.export.gov/safeharbor/sh_historicaldocuments.html (last visited Mar. 6, 2004) (under the heading "Week of March 17, 2000").

June 9, 2000,[45] and the final version July 21, 2000.[46] Also, the public was asked for comments on several occasions pursuant to the U.S. Department of Commerce's notice and comment requirement under the Administrative Procedure Act.[47] Specifically, "[t]he drafting, reception of public comments, and revisions of these 'principles' is analogous to negotiated rule making in US administrative law."[48]

These activities show that an extensive dialogue took place between the European Commission and the United States Department of Commerce. Also, the parties held a summit in Bonn on June 21, 1999. During the conference, a Joint Report on the European Union/United States Data Protection Dialogue was presented. The Report stated:

> We have made substantial progress in developing an arrangement that would provide a predictable framework for the application of the EU Directive on Data Protection to the transfer of personal data from the European Union to the United States with adequate protection for privacy. Work on the substantive aspects of data protection is particularly well advanced. On the procedural and enforcement aspects, work is also progressing but further work is needed on both sides. We plan to finalise this "safe harbor" arrangement during the autumn.[49]

However, the negotiations had not been concluded in autumn of 1999 and lasted longer than expected. Finally, on July 26, 2000, they were successfully completed and the European Commission adopted its Decision regarding the Safe Harbor Principles ("Decision

---

[45] *FAQ's*, U.S. Dept. of Commerce, *available at* http://www.export.gov/safeharbor/sh_historicaldocuments.html (last visited Mar. 6, 2004) (under the heading "Week of June 9, 1999").
[46] *Safe Harbor Documents*, U.S. Dept. of Commerce, *available at* http://www.export.gov/safeharbor/sh_documents.html (last visited Mar. 6, 2004) (under the heading "C. Frequently Asked Questions (FAQs)").
[47] *See generally* Letter from David L. Aaron, Undersecretary for International Trade of United States Department of Commerce, to U.S. organizations (Mar. 17, 2000), *available at* http://www.export.gov/safeharbor/aaron317letter.htm (last visited Mar. 6, 2004); Letter from David L. Aaron, Undersecretary for International Trade of United States Department of Commerce, to U.S. organizations (Nov. 15, 1999), http://www.export.gov/safeharbor/aaronmemo1199.html (last visited Mar. 6, 2004). To access public comments in response to the Draft Safe Harbor Principles visit http://www.export.gov/safeharbor/sh_historicaldocuments.html (last visited Mar. 6, 2004).
[48] Shaffer, *supra* note 16, at 429.
[49] Joint Report on Data Protection Dialogue to the EU/US Summit From the European Commission and the U.S. Department of Commerce (June 21, 1999), *available format* http://www.export.gov/safeharbor/jointreport2617.htm (last visited Mar. 6, 2004).

on Safe Harbor") as an adequate level of protection.[50] The Decision on Safe Harbor was adopted despite the European Parliament Resolution of July 5, 2000[51] which contested the adequacy of the protection with regard to the Safe Harbor Principles. However, the Commission justified its position, as the Parliament did not mention that the European Commission would be exceeding its powers adopting the Decision on Safe Harbor.[52]

IV. Legal Basis of the Safe Harbor Arrangement

The Safe Harbor agreement between the European Union and the United States is based on Article 25(6) of the Directive, which states that the European Commission "may find…that a third country ensures an adequate level of protection…by reason of its domestic law or of the international commitments it has entered into."[53] With regard to the United States, the European Commission adopted the Decision on Safe Harbor:

> For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the 'Safe Harbor Privacy Principles'…as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked questions…issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States.[54]

The concept is that the Safe Harbor Principles, issued by the United States Department of Commerce on July 21, 2000[55] and the accompanying Frequently Asked Questions,[56] set forth the provisions ensuring the adequate level of data protection. The Frequently Asked

---

[50] Commission Decision, The Commission of the European Communities, (July 26, 2000), 2000 O.J. (L 215) 7 [hereinafter Commission Decision].
[51] European Parliament Resolution on the Draft Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2001 O.J. (C 121) 152.
[52] Tanguy van Overstraeten & Emmanuel Szafran, *Data Protection and Privacy on the Internet: Technical Considerations and European Legal Framework*, 7 COMPUTER & TELECOMM. L. REV. 56, 63 (2001).
[53] Directive, *supra* note 1, art. 25(6).
[54] Commission Decision, *supra* note 50, art. 1.
[55] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July 24, 2000), *relevant portion available at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm (last visited Mar. 6, 2004).
[56] *Id.*, *available at* http://www.export.gov/safeharbor/sh_documents.html (last visited Mar. 6, 2003).

Questions "have the same binding force as the" Safe Harbor Principles.[57] It is not intended that the Safe Harbor Principles affect United States law, but rather to provide a so-called "safe harbor" to companies with respect to the Directive. Such companies are aware of the spill-over effects the Safe Harbor Principles may have on data protection policy and practice in the United States. Technically, United States companies are not forced to adopt them. However, businesses may do so in order to avoid restrictions on data transfer between the European Union and the United States.[58]

V. Safe Harbor Principles

A. Overview

The Safe Harbor solution sets out a number of principles with which U.S. organizations must comply if they want to receive personal data from the European Union. If a data recipient based in the United States has signed up to abide by the Safe Harbor Principles, it is assumed that an adequate level of protection will be ensured. From the standpoint of European Union businesses, a data transfer to the U.S. would be possible without significant extra efforts.[59] However, a United States organization which has not self-certified for Safe Harbor can still receive data from the European Union if one of the derogations as stated in Article 26 of the Directive would apply.[60]

According to the Decision on Safe Harbor, European Union Member States have to "take all measures necessary to comply with this Decision at the latest at the end of a period of 90 days from the date of its notification to the Member States."[61] The Decision on Safe Harbor was published in the Official Journal on August 25, 2000, which implies that the De-

---

[57] Heather Rowe, *Data Protection*, IT L. TODAY 7.10(4) (1999).
[58] Shaffer, *supra* note 16, at 429.
[59] Catrin Turner, *European Data Protection: The Challenge of International Business*, 111 COPYRIGHT WORLD 9 (2001).
[60] Directive, *supra* note 1, art. 26.
[61] Commission Decision, *supra* note 50, art. 5.

cision came into effect during November 2000. After three years of the notification, the European Commission shall in any case evaluate the implementation of the Decision on the basis of available information.[62]

B. Scope of Application

1. The Legal Basis

An organization will benefit from the Decision on Safe Harbor if:

> (a) the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs; *and*
> (b) the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate Complaints and to obtain relief against unfair and deceptive practices.[63]

Important sectors of the economy, such as telecommunications or banking, are not covered by the Safe Harbor Principles as discussed in Annex III of the Commission Decision.[64] It is also made clear by the United States Department of Commerce that "[o]rganizations that are telecommunications common carriers, meat packers, banks, insurance companies, credit unions or not-for-profits may not be eligible for Safe Harbor."[65]

There are also some exemptions with regard to journalistic material: "Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Safe Harbor Principles."[66] It is based on the United States constitutional protections for freedom of the press and the Directive's exemption for journalistic material.[67]

---

[62] Commission Decision, *supra* note 50, art. 4(1).
[63] *Id.* art. (2)(a), (b).
[64] *Id.* at Annex III.
[65] *Safe Harbor Workbook* , U.S. Dep't of Commerce, *available at* http://www.export.gov/safeharbor/sh_workbook.html (last visited Mar. 6, 2004) [hereinafter Safe Harbor Workbook].
[66] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July

2. Criticism

Important business sectors are not within the scope of the Safe Harbor arrangement. It is admitted that these sectors are excluded because the European authorities "want to hold separate negotiations with the US government over privacy protection protection in such specialized sectors."[68] However, such exclusion is not favourable to the protection of an E.U. citizen's data. For example, financial services companies are transferring data with a high degree of importance and sensitivity. Apart from the derogations as set out in Article 26 of the Directive, an overall solution needs to be found for all business sectors very soon in order to allow data transfers from the European Union to the United States.

C. First Principle: Notice

An organization must fulfill specific information requirements. An individual must be informed about the purpose of the collection and use of their personal information, how to contact the organization with regard to inquiries or complaints, the identity of any third party that such information is disclosed to, and any means and choices by which the organization limits the use and disclosure of information.[69] The language of the notice must be clear and conspicuous, and must be submitted at the time when the individual is requested to submit personal data or as soon as it is practicable.[70] In any case, the notice must be given before the information is used "for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party."[71]

24, 2000), *relevant portion available at* http://www.export.gov/safeharbor/FAQ2JournFINAL.htm (Mar. 6, 2004).
[67] *Id.*
[68] Christoph Kuner, *EU Regulations Threaten International Data Flows*, INT'L TECH. L. REV. 39, 41 (2001). Copy on file with OKJOLT.
[69] *Safe Harbor Workbook*, *supra* note 65.
[70] *Id.*
[71] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July 24, 2000), *relevant portion available at* http://www.export.gov/safeharbor/shprinciplesfinal.htm (last visited Mar. 6, 2004).

D. Second Principle: Choice

Individuals must have the opportunity to decide whether their personal information can be submitted to a third party or whether it can be used "for a purpose that is incompatible with the purpose(s) for which it was originally collected."[72] The mechanism to exercise the choice must be clear and conspicuous and readily available. In the case where sensitive information will be submitted or used in the above-mentioned way, the individual must be given an affirmative or explicit choice. Examples of sensitive information would be information revealing "medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual."[73]

However, there are some exceptions where an organization is not required to provide explicit choice with respect to sensitive data. Such a choice is, among others, not necessary:

> [W]here the processing is: (1) in the vital interests of the data subject or another person; (2) necessary for the establishment of legal claims or defenses; (3) required to provide medical care or diagnosis; (4) carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; (5) necessary to carry out the organization's obligations in the field of employment law; or (6) related to data that are manifestly made public by the individual.[74]

E. Third Principle: Onward Transfer

An organization that wishes to disclose information to a third party can only do so by applying the notice principle[75] and choice principle.[76] Where the third party to whom the information is intended to disclose "is acting as an agent," the relevant organization has to

---

[72] *Id.*
[73] *Id.*
[74] *FAQ's*, U.S. Dept. of Commerce, available *at* http://www.export.gov/safeharbor/FAQ1sensitivedataFINAL.htm (last visited Mar. 6, 2004).
[75] *See supra* Part IV.C.

ensure "that the third party subscribes to the [Safe Harbor] Principles or is subject to the Directive or another adequacy finding."[77] Also, a written agreement with such a third party, whereby the third party is obliged to ensure the same level of data protection as it is required by the relevant Safe Harbor Principles, would render the data transfer lawful. As soon as the mentioned requirements are fulfilled, the organization will not be held responsible when a third party receiving information from the relevant organization is acting in a way contrary to any restrictions or representations.[78] However, the contrary is true when "the organization knew or should have known" that the third party would transfer data "in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing."[79]

F. Fourth Principle: Security

The security principle has been drafted in one sentence. Basically, it states that an organization must take reasonable steps to prevent any loss, misuse and unauthorized access, disclosure, alteration and destruction of personal information where it creates, maintains, uses or disseminates these personal information.[80]

G. Fifth Principle: Data Integrity

The data integrity principle is in line with the requirement that "personal information must be relevant for the purposes for which it is to be used."[81] An organization is not allowed to transfer personal information in such a manner "that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual."[82] Also, an organization has to make sure that data is reliable, accurate, and complete.[83]

---

[76] *See supra* Part IV.D.
[77] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July 24, 2000), *relevant portion available at* http://www.export.gov/safeharbor/shprinciplesfinal.htm.
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] *Id.*

H. Sixth Principle: Access

An individual must have the opportunity to access personal information in the possession of the organization.[84] Also, an individual must have the right to correct, amend, or delete the information when it is incorrect.[85] This would not be the case where "expense of providing access would be disproportionate to the risks to the individual's privacy…or where the rights of persons other than the individual would be violated."[86] Apart from the Safe Harbor Principle, the United States approach interprets "access" as only covering data collected directly by the organization. The reasoning is that an organization may become liable with regard to data received "from the data subject while it is conceived as less reasonable that liability is related to data derived from other sources."[87]

However, the access principle does not specify whether or not data received from the data subject, or data collected from other sources, falls within its scope. Therefore, it can be assumed that both types would come within the scope of the principle. In the view to provide overall protection, there should not be a differentiation. It makes sense that both types are covered. Apart from that, it is admitted that organizations, which are selling publicly available information, may charge the organization's customary fee in responding to requests for access.[88] However, in order to allow individuals to freely exercise their right to access, costs should not be allocated.

I. Seventh Principle: Enforcement

Any data protection or privacy regime is effective only where mechanisms are available to ensure compliance with the data protection principles, "recourse for individuals to

---

[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] Peter Blume, *Transborder Data Flow: Is There a Solution in Sight?*, 8 INT'L J.L. & INFO. TECH. 65, 79 (2000).

whom the data relate affected by non-compliance," and consequences for the organization that does not follow the principles.[89] Minimum protection would at least ensure that a mechanism is in place which allows an investigation of the individual's complaints and disputes and also provides for an award of damages in accordance with the applicable law.[90] Also, a procedure must be established to make sure that "the attestations and assertions businesses make about their privacy practices are true" and the implemented privacy practices are still the same as they have originally been presented.[91] Finally, the organization must be required to remedy problems arising out of the failure to comply with the data protection principles.[92] Overall, the sanctions must be sufficiently rigorous to make sure that the principles will be followed.[93]

J. Criticism

The Directive specifies that a data processor has to fulfill the following basic requirements: (a) data subjects must be informed about the manner in which their personal data will be used; (b) personal data cannot be used for any other purpose that has not been communicated to the data subject; (c) individuals must have the right to correct data; (d) data subjects must be given notice before any data transference to third parties; (e) data subjects must have the option of non-participation in the collection scheme; and (f) enforcement provisions must be established in order to carryout these provisions.[94] Looking at these requirements, it can be said that the Safe Harbor Principles are basically the same as the general rules of the Directive. Also, the Safe Harbor Principle security has a counterpart in the

---

[88] *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July 24, 2000), *relevant portion available at* http://www.export.gov/safeharbor/FAQ8AccessFINAL.htm.
[89] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July 24, 2000), *relevant portion available at* http://www.export.gov/safeharbor/shprinciplesfinal.htm.
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] Long & Quek, *supra* note 7, at 333.

Directive, which sets out that "[m]ember States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against … unlawful forms of processing."[95] However, it is doubtful whether an appropriate enforcement mechanism is in place in the United States.

K. Dispute resolution and enforcement

1. Introduction

The enforcement principle sets out the requirements for safe harbor enforcement: an independent recourse mechanism is needed.[96] These mechanisms may vary, but they must be in compliance with the enforcement principle's requirements. Organizations may fulfill the requirements through the following means:

> (1) compliance with private sector developed privacy programs that incorporate the Safe Harbor Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Union or their authorized representatives.[97]

2. Recourse Mechanisms

Consumers are asked "to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms."[98] A factual question is "[w]hether a recourse mechanism is independent."[99] Several factors, such as transparent composition and financing or a proven track record, can be indicators. In every case, the resource mechanism "must be readily available and affordable."[100] Dispute resolution bodies are required to review all complaints submitted by individuals. An exception would be an

---

[95] Directive, *supra* note 1, art. 17(1).
[96] *See* Part IV.S.
[97] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July 24, 2000), *relevant portion available at* http://www.export.gov/safeharbor/FAQ11FINAL.htm.
[98] *Id.*
[99] *Id.*
[100] *Id.*

obviously unfounded complaint.[101] When individuals raise a complaint, they should obtain information about how the dispute resolution procedure works.[102]

3. Remedies and Sanctions

Any remedies provided by the dispute resolution body carries the consequence "that the effects of noncompliance are reversed or corrected by the organization" and a commitment by the organization that it will ensure compliance thereafter.[103] For instance, the organization has to make sure that future processing of personal data will be in compliance with the Safe Harbor Principles or otherwise face sanctions. Insofar as appropriate, any processing of personal data of the complainant must cease.[104] Rigorous sanctions are incorporated to ensure compliance with Safe Harbor Principles. Dispute resolution bodies may impose several sanctions in order to respond to non-compliance with the appropriate sanction. Sanctions include deletion of data obtained improperly in violation of the Safe Harbor Principles, "suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance" and/or injunctive orders.[105] Furthermore, "[p]rivate sector dispute resolution bodies and self-regulatory bodies must notify failures of safe harbor organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts."[106] Also, they are required to notify the United States Department of Commerce.[107]

L. Action by the Federal Trade Commission

Where self-regulatory organizations and European Union Member States are alleging non-compliance with the Safe Harbor Principles, the Federal Trade Commission will review

---

[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*

whether the Federal Trade Commission Act, which prohibits unfair or deceptive acts or practices, has been violated. If the Federal Trade Commission believes that a violation has occurred, "it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged" practices.[108] Essentially, the Federal Trade Commission will bring enforcement actions against violators. For example, in 1998, the Federal Trade Commission brought two actions based an alleged violations.[109] The Federal Trade Commission must inform the United States Department of Commerce whenever it takes such actions.[110]

M. Criticism

According to the Directive, Member States shall establish public authorities, which shall be responsible for monitoring the application of the relevant data protection law.[111] Each authority shall be endowed with "investigative powers," "effective powers of intervention," and "the power to engage in legal proceedings."[112] The European model is based on special supervisory powers that are quite extensive. It is not regarded "as sufficient that data subjects can use the judicial system."[113] Independent bodies are needed and they should have the necessary power and recourses in order to enforce the rules on an efficient and prompt basis as soon as they are aware of a violation. Currently in the United States, a federal authority or authorities in each State with broad powers have not been established.

---

[107] *Id.*
[108] *Id.*
[109] Shaffer, *supra* note 16, at 429 (one "action was brought against GeoCities, which has 'one of the most popular sites on the Web,'…for the alleged collection of "personal information, when the personal information was rather going directly to third parties" and the second action was brought "against Liberty Financial Companies, Inc., operator of the Young Investor Web site, for falsely representing that information collected would be maintained anonymously"). *Id.* at 429 n.36.
[110] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July 24, 2000), *relevant portion available at* http://www.export.gov/safeharbor/FAQ11FINAL.htm.
[111] Directive, *supra* note 1, art. 28(1).
[112] *Id.* art. 28(3).
[113] Blume, *supra* note 58, at 78.

Admittedly, the Federal Trade Commission Act declares "unfair or deceptive acts or practices in or affecting commerce"[114] to be unlawful and that the Federal Trade Commission would have the power to stop such acts and practices. However, the Federal Trade Commission cannot use its powers with regard to banks and savings or loan institutions. However, with regard to the financial sector, the Federal Reserve Board, the Office of Thrift Supervision, the National Credit Union Administrative Board, and the Security and Exchange Commission all have jurisdiction. Also, in practice, the Federal Trade Commission may not have a chance to take action in due time. A United States organization can benefit from the Safe Harbor arrangement at the moment it has submitted the self-certification form.[115] It can be said that the present system in the U.S. does not have a comprehensive enforcement mechanism in place. Therefore, it is difficult to argue that the enforcement of data protection rules in the United States are at the same level as the data protection rules in Europe.

Apart from that, individuals do not have a right to judicial review in case of a violation of data protection laws in all cases. According to the Directive, an individual has the right to judicial remedies “for any breach of the rights guaranteed” to them.[116] As for the United States, a system of judicial remedies needs to be established similar to those set forth in the Directive. Also, the Directive allows data subjects to claim damages for any “unlawful processing operation.”[117] The system in the United States provides for this only to a limited extent.

---

[114] 15 U.S.C. § 45(a)(1) (2000).
[115] Bargate & Shah, *supra* note 6, at 177.
[116] Directive, *supra* note 1, art. 22.
[117] Commission Decision, *id.* art. 23(1).

VI. Powers of the European Commission and the Member States

A. Decision on Safe Harbor

In case of a failure, the data protection authorities of the Member States can suspend data transfers to an organization that has self-certified its adherence to the Safe Harbor Principles. However, the following requirements must be fulfilled: (a) a U.S. government body "or an independent recourse mechanism…has determined that the organisation is violating the Principles" and (b) "there is a substantial likelihood that the Principles" result in a risk of grave harm to data subjects, which cannot be solved by means of the enforcement mechanism.[118] As soon as a data flow has been suspended, the Member States shall notify the European Commission.[119] If the European Commission shows evidence that a "body responsible for ensuring compliance with the Principles…is not effectively fulfilling its role, the [European] Commission shall inform the U.S. Department of Commerce."[120] In addition, the European Commission may draft measures with the aim of suspending or reversing the Decision on Safe Harbor.[121] Essentially, the European Commission can reverse the Decision by finding that the Safe Harbor arrangement is in adequate protection status.[122]

B. Criticism

The right and ability of the data protection authorities in the Member States to suspend data transfers is appropriate. However, the requirement that a United States government body or an independent resource has identified a violation of the Safe Harbor Principles must be fulfilled. Efficient supervisory authorities are needed to review data protection practices. However, in the United States, such supervisory authorities are only established to a limited extent. Based on this fact, the right of the European data protection authorities is

---

[118] *Id.* art. 3(1)(a), (b).
[119] *Id.* art. 3(1).
[120] *Id.* art. 3(4).
[121] *Id.*

undermined by the system in the United States. Apart from that, the European Commission may reverse the Decision. However, it is an open question whether the reversed Safe Harbor arrangement shall be replaced.

VII. Conclusion

The review of the Safe Harbor solution has identified some weaknesses. Important business sectors like telecommunications or banking are not within the scope of the Safe Harbor arrangement. An overall solution covering all business sectors needs to be found. As such, the Safe Harbor Principles are similar to the basic requirements of the Directive. However, the system of self-certification does not ensure that all companies which have joined Safe Harbor have adequately fulfilled the relevant requirements in practice. Therefore, an independent body should review the data protection regime of the organization intending to benefit from Safe Harbor. A system of data protection authorities with significant powers has not been established in the United States. The Federal Trade Commission cannot use its powers with regard to financial service organizations. Also, in practice, the Federal Trade Commission may not have a chance to take the necessary action before any personal information has been misused. It cannot be said that the enforcement of data protection rules in the United States is at the same level as it is in Europe. Individuals do not have a right to judicial review in all cases concerning a violation of data protection laws. Overall, the Safe Harbor solution cannot be regarded as the best mechanism to ensure an adequate level of protection. The enactment of appropriate data protection laws in the United States could help to close the gap and effectively ensure the adequate level of protection exists.

---

[122] Overstraeten & Szafran, *supra* note 52, at 64.