Washington Journal of Law, Technology & Arts

Volume 1 | Issue 3 Article 2

8-2-2005

Safe Harbor Agreement—Boon or Bane?

Sylvia Mercado Kierkegaard

SAFE HARBOR AGREEMENT - BOON OR BANE?

By Sylvia Mercado Kierkegaard

ABSTRACT

U.S. businesses that handle personal information about individuals living in European Union countries should be aware that, as a general rule, it is unlawful for them to transfer that data out of the European Union to the United States. Exceptions to this general prohibition apply in specified circumstances, that is, where there is consent to the transfer or where there is some assurance that U.S. businesses will comply with the transfers requirements of EU privacy laws when handling that information. These restrictions apply to U.S. businesses that have employees or customers in EU countries, as well as U.S. businesses that operate Web sites in the United States that collect information from individuals accessing their sites from the European Union. In 2000, the United States and the European Union entered into a "Safe Harbor Agreement" in order to improve U.S. businesses' compliance with EU privacy laws while minimizing the risk to U.S. businesses of enforcement actions brought against them by EU regulators for privacy law violations. U.S. businesses that decide to participate in the Safe Harbor are subject only to enforcement actions by U.S. regulators if they fail to comply with Safe Harbor requirements. Another compliance strategy open to U.S. businesses is to include standard privacy terms in contracts for transactions involving the transfer of personal information about EU individuals to the United States that provide privacy guarantees and explicitly subject the business to the jurisdiction of EU privacy regulators. In October 2004, the EU Commission released a report that reiterates the EU commitment to working with the United States within the framework of the Safe Harbor, notwithstanding the apparent lack of success of either the Safe Harbor or the contract terms compliance strategies.

TABLE OF CONTENTS

BACKGROUND

<1> More than a decade ago, major differences between the United States and European Union on the appropriate level of information privacy protection became the focus of a potentially very serious trade dispute between the United States and the European Union. The high level of legal privacy protection provided in the European Union and the comparatively low level of regulation in the United States with regard to the business use of personal information became controversial in 1995 when the European Union updated and further strengthened its information privacy law with the Council Directive 95/46 of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("Directive").[1] Of particular concern to U.S. businesses were Articles 25 and 26 of the Directive which prohibit the transfer of personal information to any country which does not ensure an "adequate" level of privacy protection. In the European Union, providing a high level of information privacy protection is considered a fundamental human right, while in the United States some businesses viewed the European Union's insistence on such high levels of protection as nothing more than a non-tariff barrier to trade. U.S. businesses that routinely transferred personal information about EU individuals to the United States, including the U.S. travel and financial services industries, worried about the financial impact of a possible European Union embargo on the transfer of personal information.

<2> In 1999, the EU Commission's independent Data Protection Working Party issued an opinion that made it clear that U.S. privacy law did not provide adequate protection, but left the door open for a diplomatic compromise that would remove the risk of enforcement actions against U.S. businesses that transferred personal information from the European Union to the United States.[2] That diplomatic compromise was

the Safe Harbor Agreement, which was put in place in 2000.[3] Since then, the EU Commission has studied the operation of the Safe Harbor and issued reports on its effectiveness in 2002 and 2004, each time finding that it has substantially failed to live up to the expectations of its drafters. Notwithstanding this disappointment, each time the European Union has reported on the operation of the Safe Harbor, it has reiterated its commitment to working with the United States within the Safe Harbor framework. As a result, U.S. businesses that transfer personal information from the European Union to the United States can still take advantage of the Safe Harbor. In addition, U.S. businesses that do not wish to join the Safe Harbor but do wish to transfer personal information from the European Union to the United States can add standard terms to their contracts setting out minimum privacy guarantees and submitting them to the jurisdiction of EU privacy regulators with regard to the transaction in question.

PRIVACY AND DATA PROTECTION

<3> Developments of a frontier free Internal Market and of the so-called "information society" have increased the cross-frontier flows of personal data between Member States of the European Union. In order to remove potential obstacles to such flows and to ensure a high level of protection within the European Union, data protection legislation has been harmonized. A regulatory framework, the Directive spells out the individual's right to have their personal data processed fairly and lawfully. The object of the Directive is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[4] and in the general principles of Community law. Adopted in 1995 and effective since 1998, it has become the de facto global standard for privacy with many nations moving to develop their own legal frameworks to ensure industry practice is compliant with EU requirements.

<4> The Directive applies "to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."[5] First, it aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down guidelines determining when this processing is lawful. The guidelines relate to: data quality; making data processing legitimate; special categories of processing; information to be given to the data subject; the data subject's right of access to data; the data subject's right to object to data processing; confidentiality and security of processing; and notification of processing to a supervisory authority. It further provides that data must be fairly and lawfully processed for limited purposes. The data must be adequate, relevant and not excessive, accurate, not kept-longer than necessary, processed in accordance with the data subject's rights, secure, and not transferred to countries without adequate protection.[6] Second, it sets out an exclusive list of lawful reasons for processing personal data. [7] Third, where "sensitive" data, such as medical data, data revealing racial or ethnic origin, or data revealing religious or philosophical beliefs, are involved, additional safeguards should be in place, such as a requirement that the person concerned explicitly consents to the processing.[8] Fourth, every person should have the right of access to personally identifiable data relating to him/her, and the right to rectify data where it is shown to be inaccurate.[9] In certain situations, he/she should also be able to object to the processing of his/her personal data.[10] Finally, the Directive contains provisions for enforcement – for government enforcement by independent agencies[11] and for private enforcement by way of judicial remedies and sanctions for any breach of a person's rights.[12]

UNITED STATES VERSUS EUROPEAN UNION APPROACH

<5> One of the most significant effects of increased online trading between Europe and the United States is the increasing concern about privacy and data protection. There is no general agreement between Europe and the United States in the area of "e-commerce" and likewise there is no specific agreement between the European Union and the United States on jurisdiction and applicable law in civil matters. Although the current consumer data privacy protection principles of the European Union and the United States are both founded upon the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued in 1980 by the Organization for Economic Co-operation and Development,[13] they are based on different approaches. The United States uses a mix of legislation, regulation, and self-regulation. Section 5 of the Federal Trade Commission Act prohibits unfair or deceptive acts or practices in the marketplace.[14] The Federal Trade Commission ("FTC") has brought a number of cases to force companies to keep the promises they make to consumers about privacy and, in particular, the precautions they take to secure consumers' personal information. Under the Financial Modernization Act of 1999, [15] the FTC has implemented rules to protect consumers' personal financial information held by financial institutions. It also protects consumer privacy under the Fair Credit Reporting Act[16] and the Children's Online Privacy Protection Act.[17]

<6> While the United States leans more heavily on a "code of conduct" for businesses, the European Union relies on the comprehensive legislation outlined above. As a result of these different privacy approaches, the Directive could have significantly hampered the ability of U.S. companies to engage in many trans-Atlantic transactions.[18] Article 25 of the Directive requires that transfers of personal data take place only

to non-EU countries that provide an "adequate" level of privacy protection, except in the cases of the derogations listed in Article 26 of the Directive. Consequently, U.S. companies could not transfer data to the United States from the European Union in a legally secure fashion. To help U.S. companies meet the "adequacy" standard, the United States and European Union agreed a solution called the *Safe Harbor*, allowing for the uninterrupted flow of personal information from the European Union to the United States by companies entering the *Safe Harbor*. The Commission adopted a Decision under which U.S. companies that agree to the Safe Harbor guidelines are regarded as being in compliance with EU privacy concerns. The U.S. companies must self-certify to the U.S. Department of Commerce their adherence to the Safe Harbor privacy principles and provide a description of their company's privacy program. Thereafter U.S. companies can exchange data between the European Union and the United States without any restriction.

SAFE HARBOR PRINCIPLES

<7> The Safe Harbor Agreement inherently involves compliance with the following criteria:

- **Notice.** Notice involves informing users, in a clear and conspicuous manner, the purpose for which information about them is collected and used; the choice mechanism available for limiting use and transfer; the types of third parties to which data is transferred; and how to contact the organization for inquiries or complaints.
- **Choice.** An organization must offer individuals the opportunity to choose (opt out) whether and how personal information they provide is used or disclosed to third parties. Opt-in choice must be available for sensitive information.[20]
- **Access**. Individuals must have reasonable access to personal information about them that an organization holds and must be able to correct that information where it is inaccurate.
- **Onward Transfer.** An organization may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice because a use is compatible with the purpose for which the data was originally collected or which was disclosed in a notice and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the Safe Harbor Principles ("Principles") or that the third party provide at least the same level of privacy protection.
- **Security.** Organizations creating, maintaining, using, or disseminating personal information must take reasonable measures to assure its reliability for its intended use and reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration, and destruction.[21]
- **Enforcement.** It requires the existence of a readily available and affordable independent recourse for individuals to whom the data relate affected by non-compliance with the principles, and, as well as consequences for the organization when the principles are not followed.
- **Data integrity**. Personal information collected must be relevant to the purposes stated in the notice, and that reasonable steps should be taken to ensure that the data is reliable, accurate, complete and current.

PROBLEMS WITH THE SAFE HARBOR

<8> Consumer groups in the European Union have voiced misgivings about the Safe Harbor Agreement because they find the U.S. data protection system inadequate when compared to the regulated system of Europe. The findings of the October 2004 EU Commission Staff Working Document[22] found that a substantial minority of U.S. businesses do not comply with the requirement of having a visible privacy policy. The Commission noted the following:

> For some of the organisations analysed, no public statement of adherence to the Safe Harbour Principles could be found. For some of the organisations, the privacy policy covered only part of the data processing indicated on the DoC certification page.18 A small number of organisations did not disclose the privacy policy on the web but ensured that it was available on the intranet. According to the information available to the Commission services, it is unknown whether such policies were indeed available on those organisations' intranet.

<9> In assessing organizations' compliance with the Safe Harbor Principles, the Commission Staff Working Document found that "[w]hile US organisations seem to make efforts to incorporate the Safe Harbour Principles into their privacy policies, as a general observation, a relevant number of the reviewed US organizations seem to have difficulties in correctly translating the Safe Harbour principles into their data processing policies."[23] The Commission considers this problematic because the Safe Harbor makes having a publicly available privacy policy mandatory and "the absence of a privacy policy or a privacy policy not

fully consistent with the Principles means that the FTC has no jurisdiction to enforce the missing Principles upon the organizations that fail to publish them.[24]

<10> While the number of organizations subscribing to the Safe Harbor has constantly increased, the number of registered organizations is lower than initially anticipated. According to the Commission Staff Working Document, 158 organizations were added to the Safe Harbor List in 2002, and another 156 in 2003. The Commission noted that without this growth in membership, "it is uncertain whether the transfer of personal data from EU-based data controllers to these organisations would have been subject to adequate protection."[25]

<11> The Commission suggests that the Department of Commerce should implement various changes to its Web site which would, among other things, enhance its transparency. Specifically, the Commission has suggested that "the [Department of Commerce] web site should provide a box for organisations to state their commitment to comply with the advice given by the EU panel in the event of a dispute without which the FTC would be unable to enforce compliance with the advice of the EU panel."[26]

<12> Safe Harbor can only apply to activities and U.S. organizations that fall within the regulatory jurisdiction of the FTC and the Department of Transportation. As a result, many companies and sectors are also ineligible for the Safe Harbor, including the banking, telecommunications, and employment sectors, which are expressly excluded from the FTC's jurisdiction.

<13> The Safe Harbor will not apply to organizations collecting data directly in Europe. Article 4 of the Directive provides that if a data controller is located outside of the European Union, but uses equipment within the European Union, the law of the place where the equipment is located will be applicable.[27] In the context of e-commerce, the substantive law of a Member State will apply rather than the Safe Harbor.

<14> An extremely important issue that does not seem to have been addressed is the cost of legal fees for European organizations seeking redress in the United States for breaches of the Safe Harbor provisions. Of particular concern is the common practice of not requiring the loser of an action to pay the reasonable legal costs of the winner.[28]

USE OF MODEL CONTRACT TERMS PROVIDED BY COMMISSION

<15> The Council and the European Parliament have given the EU Commission the power to decide, on the basis of Article 26 (4) of Directive 95/46/EC, that certain standard contractual clauses offer sufficient safeguards to the protection of privacy. Commission Decision 2001/497/EC ("Commission Decision") obliges Member States to recognize that companies or organizations using such standard clauses in model contracts concerning personal data transfers to countries outside the European Union are offering "adequate protection" to the data.[29] By incorporating the standard contractual clauses into a model contract, personal data can flow from a Data Controller established in any of the twenty-five EU Member States and the three European Economic Area (EEA) member countries[30] to a Data Controller established in a country not ensuring an adequate level of data protection. The Directive requires the following general principles to be applied:

- Personal data should be collected only for specified, explicit, and legitimate purposes; the persons concerned should be informed about such purposes and the identity of the data controller;
- Any person concerned should have a right of access to his/her data and the opportunity to change or delete data which is incorrect, and;
- If something goes wrong, appropriate remedies must be available to put things right, including compensation or damages through the competent courts.

CONCERNS ABOUT MODEL CONTRACT TERMS

<16> Under Article 26 (2) of Directive 95/46/EC, national authorities may authorize on a case by case basis specific transfers to a country not classified as offering adequate protection where the exporter in the EU cites adequate data protection safeguards. Whenever a Member State authorizes a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) of Directive 95/46/EC, it must notify the European Commission and the other Member States (Art. 26(3)). If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission must then adopt appropriate measures in accordance with the Article 31(2) procedure, which are binding on Member States. The Commission is also empowered to decide on the basis of Article 26(4) of Directive 95/46 that certain standard contractual clauses offer sufficient safeguards as required by Article 26 (2), that is, they provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. By adopting standard contractual clauses in the contract, personal data can flow from a Data Controller

established in any of the 25 EU Member States and three EEA member countries (Norway, Liechtenstein and Iceland) to a Data Controller established in a country not ensuring an adequate level of data protection. The EU model contract is intended to provide a single standard of adequate privacy protection.

<17> Under Clause 6 of the Model Contract, both the data importer and the exporter are jointly liable. Disputes can only be referred to the court of the EU Member State and the applicable law will be the data protection law where the data exporter is established.[31] In contrast, under the Safe Harbor Agreement, complainants may seek redress before a U.S.–based Alternative Dispute Resolution body. Businessmen complain that the standard clauses are not a workable alternative model. They impose unduly burdensome requirements that are incompatible with real world operations. There are clamors to make the clauses business-friendly, but the EU Data Protection Working Party insisted that any new attempts must provide added value and benefits to individuals, rather than just being more business-friendly.

<18> As a result, the Commission adopted Decision 2004/915/EC on 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries on the basis of Article 26(4) of Directive 95/46/EC. The sets of clauses adopted by the Commission in 2001 and the new set of standard contractual clauses remain fully applicable and it is up to the operators to choose the one which fits best their needs. The introduction of a new set of standard contractual clauses is intended to provide businesses with a wider choice. Some of the new clauses, such as those on litigation, allocation of responsibilities or auditing requirements, are more business-friendly. Yet they provide for a similar level of data protection as those of 2001 and to prevent abuses, the data protection authorities are given more powers to intervene and impose sanctions where necessary.

<19> The salient features of the new clauses are that they do not require the data exporter and data importer to be liable for each other's misuse of data, as was the case with the previous system of *joint and several liability* provided for in Decision 2001/497/EC. The new set contains a liability regime based on due diligence obligations where the data exporter and the data importer would be liable vis-à-vis the data subjects for their respective breach of their contractual obligations. The new set also relies on the concept of "due diligence by the data exporter". The data exporter is also liable for not using reasonable efforts to determine that the data importer is able to satisfy its legal obligations under the clauses (*culpa in eligendo*) and the data subject can take action against the data exporter in this respect.

<20> The new clauses contain more flexible and realistic auditing provisions. These reasonable efforts may include the carrying out of audits in data importers´ premises or requesting appropriate insurance coverage of any damages caused, and to request evidence of sufficient financial resources to fulfill its responsibilities (clause I (b)).

<21> The new clauses contain more flexible and realistic auditing provisions. These reasonable efforts may include the carrying out of audits in data importers´ premises or requesting appropriate insurance coverage of any damages caused, and to request evidence of sufficient financial resources to fulfill its responsibilities (clause I (b)).

<22> As regards the exercise of third party beneficiary rights by the data subjects, greater involvement of the data exporter in the resolution of data subjects' complaints is provided for, with the data exporter being obliged to make contact with the data importer and, if necessary, enforce the contract within the normal period of one month. If the data exporter refused to enforce the contract and the breach by the data importer still continues, the data subject may then enforce the clauses against the data importer and eventually sue him in a Member State (Recital 6). In order, however, to prevent abuses with this additional flexibility, it is appropriate to provide that data protection authorities can more easily prohibit or suspend data transfers based on the new set of standard contractual clauses in those cases where the data exporter refuses to take appropriate steps to enforce contractual obligations against the data importer or the latter refuses to cooperate in good faith with competent supervisory data protection authorities (Recital 7).[32]

<23> Moreover, the Commission is also working with the data protection authorities on other possible alternatives, such as "Binding Corporate Rules", that is, the use of codes of conduct instead of model contracts for the transfer of personal data to third countries. The principles of protection contained in the binding corporate rules must comply to a large extent with the principles of protection of Directive 95/46/EC. The assessment of the "binding nature" of such corporate rules implies a common assessment of their binding nature in law (legal enforceability), and of their binding nature in practice (compliance). The binding nature of the rules in practice would imply that the members of the corporate group, as well as each employee within it, will feel compelled to comply with the internal rules. The internal binding nature of the rules must be clear and good enough to be able to guarantee compliance with the rules outside the Community.

<24> Data subjects covered by the scope of the binding corporate rules must become third party beneficiaries either by the legal effects of unilateral undertakings or by contractual arrangements between the members of the corporate group making this possible. As third party beneficiaries, data subjects should be entitled to enforce compliance with the rules both by lodging a complaint before the competent data protection authority and before the competent court on Community territory. The scope of the third party beneficiary rights should match, at least the one granted by the Commission Decision 2001/947/EC

on standard contractual clauses in respect of both the Data Exporter and the Data Importer. As regards the legal enforceability of the binding corporate rules by the competent data protection authority, by submitting an application for an authorization for an international data transfer, the corporate group binds itself vis-à-vis the data protection authority to respect the safeguards adduced (in this case the binding corporate rules).

<25> The binding corporate rules should contain a clear provision indicating that where a member of the corporate group has reasons to believe that the legislation applicable to him may prevent him from fulfilling his obligations under the binding corporate rules and have a substantial adverse effect on the guarantees provided by them, he will promptly inform the headquarters in the EU or the EU member with delegated data protection responsibilities, unless otherwise prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

<26> The corporate rules should contain tailor-made provisions as well as a reasonable level of detail in the description of the data flows, purposes of the processing, etc. The level of detail must be sufficient so as to allow the data protection authorities to assess that the processing carried out in third countries is adequate. The rules are expected to set up a system which guarantees awareness and implementation of the rules both inside and outside the European Union. The applicant corporate group must also be able to demonstrate that such a policy is known, understood and effectively applied throughout the group by the employees which received the appropriate training and have the relevant information available at any moment.

<27> The rules must provide for self-audits and/or external supervision by accredited auditors on a regular basis with direct reporting to the ultimate parent's board. Data Protection Authorities will receive a copy of these audits where updates to the rules are notified and upon request where necessary in the framework of the co-operation with the data protection authority. The rules should indicate that the data subjects would benefit from the remedies and liability provided for in Articles 22 and 23 of the Directive (or similar provisions transposing these articles of the Directive in the Member States legislations) in the same way and with the same scope from which they would benefit if the processing operation carried out by the corporate group would fall under the scope of the Data Protection Directive or any national laws transposing it.

<28> The corporate group must also accept that data subjects would be entitled to take action against the corporate group, as well as to choose the jurisdiction: a) either in the jurisdiction of the member that is at the origin of the transfer, or b) in the jurisdiction of the European headquarters or the jurisdiction of the European member with delegated data protection responsibilities.

<29> In addition to the provision of information contained in Articles 10 and 11 of the Directive and national laws transposing them, corporate groups adducing sufficient safeguards must be in a position to demonstrate that data subjects are made aware that personal data are being communicated to other members of the corporate group outside the Community on the basis of authorizations by data protection authorities based on legally enforceable corporate rules, the existence and the content of which must be readily accessible for individuals.[33]

CONCLUSION

<30> Currently, U.S. organizations have only three options for establishing "adequacy" – (1) join the Safe Harbor program; (2) tailor operations to fall into an exception to the Directive; or (3) obtain approval from an EU Member State's data protection authorities for specific personal data transfer. However, these are not the only solutions for transferring data to countries without adequate privacy safeguards. Exporters can always seek the individual's unambiguous consent, or use the draft model contract option. The use of contractual clauses, though not compulsory, should offer a straightforward way of complying with data protection in the European Union. Unfortunately, the Standard Model Contract has not been widely used because it imposes significant burdens and risks. The revised model may offer greater take-up, and a specific Commission initiative on binding corporate rules may be announced in the future. For now, compliance with the Safe Harbor agreement may provide the most effective solution for U.S. businesses wishing to transfer personal information out of the European Union without violating EU law.

PRACTICE POINTERS

- In the context of a "information audit," determine if your organization handles personal information about individuals in the European Union.
- If you do handle personal information about individuals in the European Union, consider whether you are in compliance with relevant EU law: 1) Did the individuals whose data you are handling provide informed, explicit consent to the transfer of information out of the European Union? 2) Is your organization a member of the Safe Harbor or was the transfer of data governed by a contract containing a term subjecting your organization to the jurisdiction of EU privacy regulators? 3) Does your actual handling of the personal information meet the eight separate standards of EU privacy law as restated in the Safe Harbor?

- If you outsource any handling of personal information, is the transfer of information strictly limited so that the handling by the third party does not cause your organization to violate the Safe Harbor standards applicable to "onward transfers" of data?

<< Top

FOOTNOTES

1. Council Directive 95/46 of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31-39, *available at* http://www.europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (last visited Feb. 1, 2005) [hereinafter Protection of Personal Data Directive]. Under E.U. law, a "directive" creates an obligation on each Member State to enact national legislation implementing standards that conform to those defined in the directive.
2. Working Party on the Protection of Individuals with Regard to the Processing of Personal Data Opinion 1/99 of 26 January 1999 Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government, *available at* http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1999/wp15en.pdf (last visited Feb. 22, 2005)
3. United States Department of Commerce, *Welcome to the Safe Harbor*, Dec. 16, 2004, *at* http://www.export.gov/safeharbor/ (last visited Feb. 22, 2005). [hereinafter Welcome to the Safe Harbor].
4. European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 8, 213 U.N.T.S. 221 (in force Sept. 3, 1953), *at* http://www.pfc.org.uk/legal/echrtext.htm (last visited Feb 11, 2005).
5. *See* Protection of Personal Data Directive, *supra* note 1, art. 3.
6. *Id.* at art. 6, *available at* http://www.europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf (last visited Feb. 1, 2005).
7. *Id.* at art. 7.
8. *Id.* at art. 8.
9. *Id.* at art. 12.
10. *Id.* at art. 14.
11. *Id.* at art. 28
12. *Id.* at arts. 22-24.
13. Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, (1980), *at* http://www.oecd.org/dsti/sti/it/secur/prod/priv-en.htm.
14. *See* 15 U.S.C.A. § 45 (2000).
15. *See* 15 U.S.C. §§ 6801-6809 (2000).
16. *See* 15 U.S.C. § 1681 et seq. (2000).
17. *See* 15 U.S.C. § 6501 et seq. (2000).
18. *See* Welcome to the Safe Harbor, *supra* note 3.
19. Protection of Personal Data Directive, *supra* note 1, art. 26.
20. International Safe Harbor Privacy Principles, Apr. 19, 1999, www.ita.doc.gov/td/ecom/shprin.html (last visited Feb. 22, 2005).
21. This involves technologies such as encryption, access controls and physical security of the data.
22. Commission Staff Working Document SEC (2004) 1323 of 20 October 2004 on the Implementation of Commission Decision 520/2000/EC on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/sec-2004-1323_en.pdf#search='October%202004%20Commission%20staff%20working%20document%20SEC%20(2004)%
' (last visited Feb. 22, 2005) [hereinafter Commission Staff Working Document].
23. *Id.* at 7.

24. *Id.* at 13.
25. *Id.* at 5.
26. *Id.* at 13-14.
27. Protection of Personal Data Directive, *supra* note 1, art. 4.
28. Graham Lea, *US-Europe privacy deal: agreeing to ignore it?*, The Register, Mar. 16, 2000, http://www.theregister.co.uk/2000/03/16/useurope_privacy_deal_agreeing/ (last visited Feb. 22, 2005).
29. Commission Decision 2001/497/EC of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, Under Directive 95/46/EC, 2001 O.J. (L 181) 19-31, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_181/l_18120010704en00190031.pdf (last visited Feb. 22, 2005) [hereinafter Commission Decision on Standard Contractual Clauses].
30. Member countries include Norway, Liechtenstein and Iceland.
31. *Id.* at clause 7.
32. Available at http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm (last visited April 15 , 2005).
33. . Details available at: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp74_en.pdf (last visited April 15 , 2005)

<< Top