DATA PROTECTION

The EU has broad and extensive protections for personal data. Both the member states and EU institutions are subject to data protection legislation, and these provisions are far more extensive than privacy legislation in the United States. While the EU regulates all private entities and governmental institutions that process personal data, data protection legislation in the US is limited to only some sectors, such as education records, consumer credit reports, and health care provider records.[1] Moreover, EU requirements are generally more stringent than US requirements regarding the same types of information.

The extensive protection given to personal data in the EU reflects a long tradition of protecting personnel privacy in Europe. There are explicit privacy rights in the constitutions of most European countries and in Article 8 of the European Union Charter of Fundamental Rights, which provides, "Everyone has the right to respect for private and family life, his home, and his correspondence."[2] Moreover, as compared to the common law, the civil law has been more protective of privacy rights. As well, significant government involvement in private markets is more traditional in Europe than in the United States, paving the way for data protection regulation of private entities. Finally, and importantly, the European concern for data protection also reflects the cruel and immoral misuse of personal data in Germany to locate and deport to concentration camps millions of Jews and other victims of the Holocaust.[3]

This chapter examines the protection of personal data in the EU. The discussion focuses on the regulatory processes used to protect personal data and the institutions that implement these protections. The chapter also considers three developments which have affected the implementation of privacy regulation in the EU. Member states in the EU have differed in their implementation of privacy directives, which creates problems for ensuring effective implementation of the directive and maintaining an integrated market in the EU.[4] In addition, the effort to protect personal data has also come into conflict with promoting transparency in EU and member state institutions when data access would reveal personal data about EU residents. Finally, efforts protect personal data have conflicted with international trade because the EU seeks to ensure that personal data relating to EU residents which is transferred out of the EU receives an adequate level of protection.

---

[1] Family Education Rights and Privacy Act (1974) (codified at 20 U.S.C. §1232g); Fair Credit Reporting Act (1970) (codified at 15 U.S.C. §1681 et. seq.); Right to Financial Privacy Act (1978) (codified at 12 U.S.C. 3401 et. seq.); Health Insurance Portability and Accountability Act (2002) (codified at 42 U.S.C. §210).

[2] ECHR art. 8(1), available at http://www.hri.org/docs/ECHR50.html#C.Art8.

[3] Marsha Huie, Stephen F. Laribee, & Stephen D. Hogan, *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 441 (2002).

[4] *See* Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L L. 807, 834-846 (2005) (describing differences among EU Member States).

DIRECTIVE 95/46

The EU has promulgated two directives in an effort to harmonize the protection of personal data in the member states and facilitate integration of the internal market.[5] Directive 95/46[6] establishes the obligation of the EU national authorities to regulate the "processing" of "personal data" by government and private entities, and it specifies some of the elements of the administrative process member states must use. Directive 2002/58 addresses the processing of personal data in the electronic communications sector.[7] Directive 95/46 is discussed first followed by a discussion of Directive 2002/58.

Personal Data

Directive 95/46 applies to the "processing" of "personal data" by "controllers." Personal data is "any information relating to an identified or identifiable natural person," known as a "data subject." The term "personal data" includes all information about a person, not only information about the person's private life, such as economic and professional information.[8] Information relates to a data subject when that the information "can be identified, directly or indirectly" with a specific person. This includes when the person can be identified "by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[9] The Directive indicates that "in order to determine whether a person is identified … account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify said person …."[10] Thus, the Directive protects any set of data, which if taken together, would make it possible to match personal data to a particular individual or to make it easier to identify that person.[11]

Despite the broad definition of "personal data," member states have disagreed how to determine when data "identifies" a person entitling that person to the protections mandated by the Directive.[12] These disagreements focus on how probable it must be that someone can determine a person's identify from the information in question. Should, for example, the issue be resolved by considering the data itself, the data and other information in possession of the data user, or by considering whether there is any possibility that the information in question can be traced back to the data subject?[13]

---

[5] Report from the Commission, First report on the implementation of the Data Protection Directive (95/46/EC) (2003), at 1, available at http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0265en01.pdf.
[6] Council Directive 95/46, 1995 O.J. (L 281) 31.
[7] Council Directive 2002/58/EC, 2002 O.J. (L201) 37.
[8] *Id*. at 50.
[9] Council Directive 95/46, *supra* n. __, at art. 2(a).
[10] Council Directive 95/46, *supra* n. __, at recital 26.
[11] CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW & ONLINE BUSINESS 5 (2003)
[12] Joel Reidenberg & Paul M. Schwartz, Data Protection Law and Online Services: Regulatory Responses 122 (1998), available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/regul_en.pdf.
[13] *See id*. (describing differences among member states).

Data Processing

A controller engages in "processing" any time there is "any operation, or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[14] A controller includes any "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data …."[15] Since both governmental and private entities are "controllers" which "process" personal data according to these definitions, Directive 95/46 obligates national authorities to regulate the use and disclosure of personal data by both government and private entities.

The *Lindqvist* case[16] confirms and illustrates the broad manner in which "controller" and "process" are defined. In *Lindqvist*, the European Court of Justice (ECJ) found that the posting of information about the members of a church by another member of the church on an internet home page constituted the "processing" of "personal data." The web site contained the names of various individuals, their jobs, hobbies, telephone numbers, and in one instance, that a person had injured her foot.

Acquisition, Maintenance, and Accuracy

Directive 95/46 requires national authorities to ensure the following protections are available to data subjects concerning the acquisition, maintenance and accuracy of personal data. First, controllers are prohibited from acquiring personal data except for "specified, explicit and legitimate purposes," and they cannot process such data in any way incompatible with those purposes.[17] Second, controllers are obligated to ensure the accuracy and completeness of such records, destroy personal data after it is no longer needed for a legitimate purpose,[18] and implement appropriate technical and organizational measures to protect personal data against unlawful destruction or accidental loss, alteration, [and] unauthorized disclosure or access …."[19] Controllers are also required to notify the member state prior to the processing of certain types of personal data,[20] but member states can simplify or eliminate this requirement under several conditions,[21] including when the controller appoints a "personal data protection official" responsible for ensuring compliance with the laws and regulations of the national authority.[22] The member states have taken advantage of this exception, producing variation from country to country concerning when notification is not

[14] *Id*. at art. 2(b).
[15] Council Directive 95/46, *supra* n. __, at art. 2(d).
[16] Case C-101/01, Criminal Proceedings Against Bodil Lindqvist, 2003 ECR I-12971.
[17] *Id*. at art. 6.
[18] *Id*. at art. 6.
[19] *Id*. at art. 17.
[20] *Id*. at art. 18-19.
[21] *Id*. at art. 18.2-18.5
[22] *Id*. at art. 18.2.

necessary.[23] Finally, controllers must provide data subjects with detailed information about what personal data they have about an individual,[24] and data subjects have the right to see such data, rectify errors or erase or block erroneous information,[25] seek judicial review of the breach of any rights, and receive compensation for any damages.[26]

Consent

Directive 95/46 also protects data subjects by requiring controllers to obtain consent for the processing of personal data unless the processing fits within one of the exceptions to requiring consent.[27] Since "processing" includes the disclosure of personal data,[28] a data controller cannot disclose personal data without the consent of the data subject or unless one of the exceptions to the need for consent applies.

The type of consent required depends on the nature of the information being processed. A controller must have "explicit" consent of the data subject to process information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and concerning health or sex life.[29] To process other types of information the controller must obtain the "unambiguous" consent of the data subject.[30] In order to "consent," the data subject's agreement to the processing of data relating to him or her must "freely given," "specific" and "informed."[31] Because consent must at least be "unambiguous," the Directive restricts the use of long, complicated, and non-transparent consent forms,[32] such as clicking "yes" on a Web site where the standard terms and conditions of the person is accepting are located somewhere else on the site under several layers of hyperlinks.[33]

The definition of "consent" does not specify whether it must be on an "opt-in" basis, where the data subject takes some affirmative action, such as checking a box on an electronic form, or on an "opt-out" basis, where the data subject consents by failing to take some action, such as by failing to click a box on an electronic form. This matter is therefore left for national authorities to decide as it relates to specific situations,[34] and national laws and regulations differ. For example, countries have adopted different requirements concerning what constitutes adequate consent in the employment context,[35]

---

[23] Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union adopted on 18 January 2005, at 8, 10211/05/EN WP 106, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp106_en.pdf.
[24] *Id*. at art. 10-11.
[25] *Id*. at art. 12.
[26] *Id*. at art. 22-23.
[27] *Id*. at art. 7.
[28] *See* note __ & accompanying text.
[29] Directive 95/46, *supra* note __, at art. 8.2(a).
[30] *Id*. at art. 7(a).
[31] *Id*. at art. 2(h).
[32] Rehder & Collins, *supra* n. __, at 134.
[33] KUNER, *supra* n. __, at 68.
[34] *Id*.
[35] Rehder & Collins, *supra* n. __, at 158-59.

and the Commission is considering whether an additional directive concerning employment information may be necessary to harmonize the regulatory approach to this issue.[36] Since, however, there must be "explicit" consent to processing of "sensitive" personal data, a controller cannot use an "opt-out" system of approval for this type of information.[37]

Exceptions

As noted, the Directive establishes a number of exceptions that permit the processing of personal data without the consent of the data subject. A controller, for example, can process personal data, if it is "necessary" for the performance of a contract to which the data subject is or will be a party.[38] A controller can also process such information if is "necessary" to comply with a legal obligation of the controller, protect the vital interests of the data subject, perform a task carried out in the public interest, or if it is "necessary" for the purposes of other legitimate interests except where such interests are overridden by the interest of the data subject in personal privacy.[39] National data authorities have reached different conclusions concerning when data processing is "necessary" according to these exceptions, which can be explained in part by differences in business practices in these countries.[40]

The Directive has additional exceptions to the ban on processing personal data without consent of the data subject. A controller, for example, does not need consent to process personal data if it involves "operations concerning public security, defence, State security … and the activities of the State in areas of criminal law" or if the processing is "by a natural person in the course of a purely personal or household activity."[41] In the *Lindquist* case, discussed earlier, the ECJ held that the establishment of the church website containing personal data did not qualify for the latter exception because the church bulletin revealed information about persons other than the author of the bulletin.[42]

The Directive also requires member states to provide for exceptions for the processing of personal data "carried out solely for journalistic purposes or the purpose of artistic or literary expression," but only if "they are necessary to reconcile the right to privacy with the rules governing freedom of expression."[43] In *Lindquist*, the controller had argued that the creation of the church website was protected by general principles of freedom expression, and therefore permitted until this clause. The ECJ replied that the national authorities and courts were "responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in

---

[36] *See* Commission Second State Consultation of Social Partners on the Protection of Workers' Personal Data, available at http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultationdataprot_en.pdf.
[37] KUNDER, *supra* n. __, at 68; Jörg Gehder & Ericka C. Collins, *The Legal Transfer of Employment-Related Data to Outside of the European Union: Is It Even Still Possible*?, 39 INT'L LAW 129, 136 (2005).
[38] *Id*. at art. 7(b).
[39] *Id*. at art. 7(c)-(f).
[40] *See* Rehder & Collins, *supra* n. __, at 134-36 (providing examples).
[41] Council Directive 95/46, *supra* n. __, at art. 3.
[42] Lindquist, note __ *supra*.
[43] Council Directive 95/46, *supra* n. __, at art. 9.

question, including the fundamental rights protected by the Community legal order," and it reserved the resolution of that issue in this case for the national courts.[44] Since member states are responsible for determining when the freedom of expression overrides the protection of personal data, there is considerable variation in national laws concerning data protection and the media.[45]

Regulatory Institutions

Directive 95/46 not only establishes the type of protections a national authority must adopt, it also requires the adoption of "suitable measures to ensure full implementation" of the directive and to establish "suitable sanctions" for infringement of data protection legislation.[46] Besides this general edict, the Directive takes three additional steps. First, it obligates a member state to establish a "supervisory authority," which has the power to conduct investigations, to order the blocking, erasure or destruction of illegal data processing, and the authority to engage in legal proceedings to effectuate its orders.[47] This national privacy authority, which must "act with complete independence in exercising its functions,"[48] is also obligated to receive complaints alleging the breach of privacy rights from individuals or associations that represent such individuals.[49] Second, a member state must also provide a judicial remedy for the unlawful processing of information, including the right to receive compensation for any damages a person might suffer.[50]

Third, Article 29 of the directive establishes an advisory "Working Party on the Protection of Individuals with Regard to the Processing of Data."[51] The "Article 29 Working Party" is composed of a representative from each member state from its supervisory authority, a representative of the Commission, and a representative of the EU Data Supervisor. It issues interpretive documents which can be influential since they are often used by national courts and national data privacy authorities.[52] Nevertheless, the working papers are not legally binding since the role of the Working Party is only advisory.[53] Despite its potential influence, meetings of the Working Party are closed, and it does not publish its agenda.[54]

DIRECTIVE 58/2002

[44] *Lindquist*, *supra* n. __, at ¶90.
[45] KUNER, *supra* n. __, at 76; *see* Art. 29 Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, Recommendation 1/97 on Data protection law and the media (Feb. 25, 1997), available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1997/wp1_en.pdf.
[46] Council Directive 95/46, *supra* n. __, at art. 24.
[47] *Id*. at art. 28.1.
[48] *Id*.
[49] *Id*. at art. 28.4.
[50] *Id*. at art. 22-23.
[51] *Id*. at art. 28.
[52] KUNER, *supra* n. __, at 10.
[53] *Id*.
[54] *Id*.

Since Directive 95/46 applies to any processing of personal data, it regulates the processing of personal data in the communications sector. In 2002, however, the Council approved Directive 58/2002[55] to address unique problems in electronic communications services, such as spam e-mails and the uses of cookies or spy-ware. Directive 58/2002 applies to personal data processed in "publicly-available electronic communications services in public telecommunications networks in the Community."[56]

Directive 58/2002 takes precedence over Directive 95/46 whenever one of its mandates is applicable,[57] although how the two directives interact concerning some issues is not yet clear.[58] It is clear, however, the directive requires member states to enact regulatory requirements that are unique to the electronic communications sector, such as additional obligations to safeguard personal data. Controllers must "ensure a level of security appropriate to the risk presented" taking into account "the state of the art and the cost of [implementation of such measures]" and to notify subscribers of the extent to which the risk of unauthorized disclosure is not eliminated by the measures taken by the controller.[59] The directive also regulates unsolicited communications, which are only permitted with opt-in consent,[60] except that businesses can send unsolicited communications to their existing customers on an opt-out basis.[61] Further, member states must permit the use cookies and other types of spy-ware, but only if data subjects are given clear and comprehensive information about the purposes of the processing related to the use of these devices and have the opportunity to opt-out of such uses.[62]

MEMBER STATES

The ambitious agenda to protect personal data established by the data privacy directives has been affected by two developments in the member states. Like other directives, this one left many of the details to be decided by the member states, producing both different interpretations of some regulatory requirements and different levels of enforcement. These differences impact both the level of privacy protection in the EU and the movement of goods between member states.

An EU website provides links to the legislation passed in each member state.[63] In addition, the Commission has a series of reports on data protection which contain a

[55] Council Directive 2000/58, *supra* n. __.
[56] Council Directive 2000/58, *supra* n. __, at art. 3(1).
[57] KUNER, *supra* n. __, at 23-24.
[58] *See* Frederic Debusseré, *The EU-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?*, 13 INT'L J.L. & INFO. TECH. 70, 81 (2005) (describing interpretive problems).
[59] *Id*. at art. 4.
[60] *Id*. at art. 13(1).
[61] *Id*. at art. 13(2). The Directive leaves it to Member States to determine whether to use opt-in or opt-out consent for other types of unsolicited communications. *Id*. at art. 13(3).
[62] *Id*. at art. 5(3).
[63] Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data, available at http://europa.eu.int/comm/justice_home/fsj/privacy/law/implementation_en.htm#belgium.

description of legislative and regulatory developments in each member state during the time period covered by the report.[64]

This information reveals that member states have different policy positions on some data protection issues, and that member states have adopted different procedural protections.[65] Some of these differences have been noted earlier. Likewise, attitudes towards enforcement vary in the Member States, with some national data protection authorities taking proactive approaches and other authorities reserving formal proceedings for particularly egregious cases.[66]

Divergences among member states can threaten the goal of harmonizing data protection regulation in order to facilitate a common market. At the same time, the divergences often reflect the varying policy viewpoints in the member states concerning the data protection. One of the functions of the Article 29 Working Group is to recommend how some of the differences in approach should be reconciled. The Working Group, for example, has addressed issues such as how member states have utilized exceptions to the requirement that controllers notify the national data authority prior to processing personal data,[67] the varying enforcement activities of member states,[68] and varying approaches to regulating the processing of persona data in employment contexts.[69]

TRANSPARENCY

Another problem concerns data protection and data access. The data protection directives reflect the understanding in the EU that data protection is of fundamental significance, but so is government transparency. This section considers two potential conflicts between data protection and governmental transparency. The first conflict arises when a national authority publishes information that includes personal data. The second conflict arises when an individual seeks information under a data access law that includes personal data.

---

[64] *See, e.g.*, European Commission, Seventh report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the years 2002-2003 (2004), available at http://www.statewatch.org/news/2005/feb/7th-rep-data-prot-02-03.pdf; European Commission, Sixth annual report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the years 2001 (2003), available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/2003-6th-annualreport_en.pdf.

[65] Bignami, *supra* n. __, at 827; see KUNER, *supra* n. __, at 12-16 (describing differences in procedural protections among the Member States).

[66] KUNER, *supra* n. __, at 41.

[67] *See* notes _ & accompanying text.

[68] Article 29 Data Working Party, Declaration of the Article 29 Working Party on Enforcement adopted on 25th of November 2004, 1206704/EN WP 101, available at http://www.datenschutz-berlin.de/doc/eu/gruppe29/wp101/wp101_en.pdf.

[69] Opinion 8/2001 on the processing of personal data in the employment context adopted on 13 September2001, 5062/01/EN/Final WP 48, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf.

In both cases, Article 7(c) of Directive 95/46 is applicable. Article 7(c) authorizes the processing of personal data when it is "necessary for compliance with a legal obligation to which the controller is subject."[70] Since Article 7(c) appears to authorize the disclosure of personal data whenever another law requires it, it appears to authorize the disclosure of personal data whenever another law requires its publication or its disclosure pursuant to a data access request. Article 7(c), however, has been interpreted to limit the authority of member states to pass such legislation.

Published Information

In the *Österreichischer Rundfunk and Others* case,[71] the ECJ considered the application of Article 7(c) to a German law which required a large number of governmental bodies to disclose publicly the salaries and pensions of officials earning more than a certain amount of money. After finding the information was "personal data" within the scope of Directive 95/96,[72] the Court found that the disclosure of such information would be legitimate only if "such publicity is necessary and proportionate to the aim of keeping salaries within reasonable limits" and only if "the objective could not be attained equally effectively by transmitting the information as to names to the monitoring bodies alone,"[73] both of which were issues to be determined by the German courts.[74] The ECJ also found that if the national courts concluded that disclosure of such data did not satisfy the previous tests, it could not satisfy Article 7(c) of Directive 95/96.[75]

Data Access Laws

The Working Group has proposed a similar interpretation of Article 7(c) as it applies to data access laws. The Working Group interprets Article 7(c) as limiting the authority of member state to authorize disclosure of personal data in domestic data access legislation because, although Article 7(c) creates an exception for compliance with a law, a member state is still required to comply with Directive 95/46.[76] If, therefore, a member state had a public access law that did not have an exception for privacy interests, the member state would be in violation of the Directive 95/46 since it would in the position of permitting the disclosure of personal data without regard to the protections required by Directive 95/46.[77]

---

[70] Directive 95/46, *supra* n. __, at Art. 7(c).
[71] Judgment of the Court of 20 May 2003 in Joined Cases C-465/00, C-138/01 and C-139/01, OJ 2003 C171/3, Jul 19, 2003.
[72] This aspect of the case is discussed later in the chapter. *See infra* notes __ & accompanying text.
[73] *Österreichischer Rundfunk and Others*, *supra* n. __, at ¶88.
[74] *Id*. at ¶90.
[75] *Id*. at ¶91.
[76] Data Protection Working Party, Opinion 5/2001 On the European Ombudsman's Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH, WP 44, 5003/00/EN/Final (May 17, 2001), available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp46en.pdf.
[77] Data Protection Working Party, Opinion 5/2001 On the European Ombudsman's Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH, WP 44, 5003/00/EN/Final (May 17, 2001), at 5, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp46en.pdf.

According to the Working Party, Article 7(f) confirms the previous interpretation.[78] Article 7(f) authorizes the disclosure of personal data "as necessary for the legitimate interests pursued by the controller … except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject under Article 1(1)."[79] Article 1(1) obligates member states to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of data."[80]

Finally, the Working Group concludes Articles 7(c) and 7(f) imply that the conflict between the Directive and legislation on public access must be resolved on a case-by-case basis, "in order to conclude which of the two rights or interests should prevail [in] each particular circumstance, and therefore whether the request for access should be satisfied or rejected."[81] The Working Group warns, however, that member states should be aware that sensitive types of personal data are the subject of heightened protection under the Directive and are therefore entitled to enhanced protection under a balancing approach.[82]

EXTRA-TERRITORIAL APPLICATION

The previous development concern activities and conduct within the EU. The EU, however, has given extra-territorial effect to its data privacy requirements to ensure that controllers cannot evade the regulatory requirements by moving processing operations to a non-EU or "third" country. The effort to implement this part of the directive has been problematic because there is a conflict between the EU's interest in facilitating international trade and its interest in providing broad protection of personal data. This section discusses the extra-territorial application of the data privacy directives, the regulatory process used to implement this requirement, and the controversies that have arisen concerning these efforts.

Directive 95/46 has extra-territorial application between it forbids the transfer of personal data to a third country until there is a determination that it has an "adequate level of protection" for such information.[83] The EU has determined that only a few countries meet this test, and that the United States is not one of them. The transfer of personal data to the US is therefore banned unless a controller can rely on one of four exceptions.

---

[78] Data Protection Working Party, Opinion 5/2001 On the European Ombudsman's Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH, WP 44, 5003/00/EN/Final (May 17, 2001), at 6, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp46en.pdf.

[79] Council Directive 95/46, *supra* note __, at art. 7(f)..

[80] *Id*. at art. 1(1).

[81] Data Protection Working Party, Opinion 5/2001 On the European Ombudsman's Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH, WP 44, 5003/00/EN/Final (May 17, 2001), at 5, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp46en.pdf.

[82] *Id*.

[83] Council Directive 95/46, *supra* note __, at art. 25.

Personal information can be transmitted to an organization that has engaged in a self-certification process established pursuant to a Safe Harbor agreement between the EU and the US. Airlines can transfer certain types of passenger data as specified in another EU-US agreement. Personal data can also be transferred outside of the EU if a controller adopts model contract provisions issued by the EU or agrees to obey a Code of Conduct approved by the EU.

Adequate Level of Protection

Directive 95/96 makes national privacy authorities responsible for determining whether a country has an adequate level of protection, and if a country lacks such protections, a national authority must block information transfers to that country.[84] A member state can also determine adequacy on an *ad hoc* basis by approving a particular data transfer.[85] The data privacy authority is also obligated to report any finding that a country lacks adequate protections to the Commission,[86] which has three options. It can affirm the decision of the member state, negotiate with the country to achieve an adequate level of protection, or initiative action to block data transfers from all member states.[87] In taking any of these actions, the Commission must consult a comitology committee of Member State representatives[88] and seek the opinion of the Working Party,[89] which as noted earlier, is made up of representatives from the member state privacy authorities.[90]

Despite these procedures, the Commission has been largely responsible for making adequacy determinations. No member state has decided on its own to block a data transfer,[91] apparently because of the potential political ramifications.[92] At the same time, no member state has approved a country's laws as being adequate either.[93] Instead, the Commission has on its own approved some countries as having an adequate level of data protection (Argentina, Canada, Isle of Man Guernsey, and Switzerland),[94] has considered

---

[84] The Directive requires a member state to assess the adequacy of a country's data protection laws

> in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Id. at art. 25.2.

[85] KONER, *supra* note __, at 134.

[86] *Id*. at 25.3.

[87] *Id*. at art. 25.4-6.

[88] *Id*. at art. 26.3-4.

[89] *Id*. at art. 30.1(b).

[90] *See* notes _ & accompanying text.

[91] See Francesca Bignami, *Transgovernmental Networks Vs. Democracy: The Case of the European Privacy Network*, 26 MICH. J. INT'L L. 807, 832 (2005).

[92] KONER, *supra* note __, at 133.

[93] *Id*.

[94] EU, Commission decisions on the adequacy of the protection of personal data in third countries, available at http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm.

other countries for approval, and has engaged in bi-lateral negotiations with other countries to obtain additional safeguards.[95]

Exceptions

If a country does not have adequate laws to protect personal data, a national privacy authority can still permit the transfer of data if the controller meets one of the exceptions in the Directive. Data transfers are permitted when the data subject has unambiguously consented to the proposed transfer.[96] If there is no consent, a data transfer is still possible if it necessary to perform a contract between the data subject or to the implementation of pre-contractual measures requested by the data subject. A transfer is also legal when it is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims, necessary in order to protect the vital interests of the data subject, or the transfer is from a data base to which the public in the member state has access according to national laws on data access.[97]

Finally, Directive 95/26 permits the transfer of data to a third country when the recipient of the data agrees to provide sufficient protection in a contract or by other means.[98] If a national privacy authority approves the transfer of personal data pursuant to this exception, it must notify the Commission and other member states of its approval.[99] If the Commission or a member state objects to the transfer, the Commission will make a final decision whether to approve the data transfer.[100] Before taking this decision, the Commission must consult the comitology committee[101] and seek to opinion of the Working Party,[102] as it is required to do concerning member state actions that block the transfer of personal data.

Implementation

EU officials have expressed concern about the lax enforcement of the ban on transferring personal data to third countries which do not have adequate levels of data protection. In a report in December 2003, the Commission concluded "[m]any unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate

---

[95] Bignami, *supra* note __, at 831.
[96] Council Directive 95/46, *supra* note __, at art. 26.1.
[97] *Id*.
[98] Council Directive 95/46, *supra* note __, at art. 26.2. According to the Directive:

> a Member State may authorize 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), where the controller adduces 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; such safeguards may in particular result from appropriate contractual clauses.

Id. at art. 26.2.
[99] *Id*. at art. 26.3.
[100] *Id*. at art. 26.3.
[101] *Id*. at art. 26.3-4.
[102] Council Directive 95/46, art. 30.1(b), 1995 O.J. (L 281) 31, __.

protection."[103] This conclusion was based in part on the small number of notifications that the Commission had received from member states that they had approved contract provisions as providing sufficient data protection. As Professor Bignami has observed, the small number of notifications "in light of the volume of trade between the European Union and the rest of the world, much of which does not follow the European approach to information privacy," makes it "difficult to believe that European's privacy is protected when their data is transferred abroad."[104] Two other observers concur finding it "is a well-known secret that, even though member states have the authority to impose sanctions on companies breaching the data privacy laws, the enforcement of these laws have been relatively lax to date."[105]

The limited number of notifications may attributable to the use by controllers of the Article 26(1) exceptions since these exceptions, when they apply, permit the transfer of data to third countries with inadequate protections. As a result, if controllers are utilizing these exceptions, there is no need for a country to rule on the adequacy of the protections in the country to which the data are being sent. The Article 29 Working Party has found that member states have adopted significantly differing interpretations of Article 26(1), which has enabled controllers to engage in "forum shopping among Member States, depending on how loosely these provisions are being interpreted."[106] The Committee has responded by recommending that national authorities should narrowly construe the exemptions, but since this recommendation may be at odds with the interest of member states in facilitating international commerce, it also stressed the importance of harmonizing how member states interpret the exceptions.[107]

Safe Harbor Agreement

Directive 95/46, as noted in the last section, permits the transfer of data to a country with inadequate data protection if a data controller furnishes adequate safeguards using contractual clauses or other means. The US[108] and the EU[109] have taken advantage of this provision to reach a Safe Harbor agreement which establishes a process for United States companies to qualify for the transfer of personal data from the EU. Firms in the United States which agree to abide by the data protection principles in the agreement are presumed to qualify for this exception.

---

[103] Report from the Commission: First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, at 19, available at http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0265en01.pdf.
[104] Bignami , *supra* note __, at 834.
[105] Rehder & Collins, *supra* note __, at 157.
[106] Working document on a common interpretation of Article 26(1) of Directive 95/46/EC: Version of 24 October 1995, 2093/05/EN WP 114, at 3, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf .
[107] *Id*. at 17.
[108] Department of Commerce, Issuance of Safe Harbor Principles and Transmissions to the European Commission, 65 Fed. Reg. 45666 (2000).
[109] Commission Decision 2000/520, 20000 O.J. (L21) 5, available at http://personuvernd.is/tolvunefnd.nsf/Files/2000_520_EC/$file/2000_520_EC.pdf.

The agreement was not easily reached. Not only were there were long and protracted negotiations, the Commission adopted the agreement despite a 279 to 259 vote in the EU Parliament which endorsed a report of a consumer rights committee critical of the adequacy of remedies in the agreement.[110] The Commission was not bound by the vote because Parliament's powers were limited to determining whether the Commission had failed to follow proper procedures in negotiating and drafting the Safe Harbor agreement. The Commission, however, did reserve the right to re-think the framework of the agreement if the fears of the Parliament turned out to be accurate.[111]

The details of the safe harbor process are found in the safe harbor principles,[112] a set of frequently asked questions (FAQs) and responses,[113] the Commission decision approving the agreement,[114] and various other documents relating to the agreement.[115] The FAQ's, according to the Department of Commerce, are intended to serve as "authoritative guidance" concerning implementation of the principles.[116]

An organization can indicate its intent to comply with the principles in three ways.[117] It can join a self-regulatory privacy program that adheres to the principles, develop its own self-regulatory privacy policies which conform to the principles, or it can agree to abide by the principles in a written agreement with parties transferring data from the EU. In addition, organizations subject to a statutory, regulatory, administrative or other body of law (or of rules) that effectively protects personal privacy may also qualify for safe harbor benefits.[118] To be eligible for the safe harbor presumption, organizations must self-certify to the Department of Commerce its adherence to the principles.[119]

The Principles, which are similar to the mandates in Directive 95/46, establish seven obligations:[120]

- *Notice***:** An organization must inform a data subject about the purposes for which it collects and uses personal information, how the data subject can contact the organization with any inquiries or complaints, whether the information will be transmitted to third parties, and what options the organization offers the data subject for limiting the use and disclosure of personal data.

---

[110] Marsha Cope Huie, Stephen F. Laribee, & Stephen D. Hogan, *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 319, 448 & 448 n. 208 (2002).
[111] *Id*. at 448.
[112] Safe Harbor Privacy Principles, available at http://www.export.gov/safeharbor/sh_documents.html.
[113] *Id*.
[114] Commission Decision 2000/520, *supra* note __.
[115] See Department of Commerce, Documents and Public Comments Provided through the Duration of the Safe Harbor Negotiations (November 1998 - June 2000), available at http://www.export.gov/safeharbor/sh_historicaldocuments.html.
[116] Department Commerce, *supra* note __, at 45,666.
[117] *Id*.
[118] *Id*.
[119] FAQ 6 - Self-Certification, available at http://www.export.gov/safeharbor/FAQ6SelfCertFINAL.htm.
[120] Principles, *supra* note __.

- *Choice*: An organization must offer the data subject the opportunity to block the disclosure of personal data to third parties, the processing of personal data which is incompatible with the purpose for which it was originally collected, and the use of personal data for purposes which have not been authorized by the data subject. An organization can meet the previous commitments by establishing an opt-out system, but it cannot disclose sensitive data without the express permission of the data subject (i.e., an opt-in system) with some exceptions.[121] In all circumstances, data subjects must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise these rights.

- *Data Transfers*: An organization may transfer personal data to a third party acting as its agent without violating Directive 95/46 in any of the following circumstances: the agent subscribes to the Safe Harbor Principles, is subject to Directive 95/46, is subject to a legal regime found to be adequate by the EU, or the agent enters into a written agreement with the organization that it will provide at least the same level of privacy protection as is required by the relevant Principles. The organization, however, may not transfer personal information to an agent in any of the previous circumstances if it knew or should have known the agent would process the information in a manner inconsistent with the Principles and the organization failed to take reasonable steps to prevent or stop such processing.

- *Security*: An organization creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

- *Data integrity***:** An organization must not process personal information in ways that are incompatible with the purposes for which it has been collected or in ways that data subject has authorized. An organization must also reasonable steps to ensure that data is reliable for its intended use and that it is accurate, complete, and current.

- *Data Access***:** An organization must give data subjects access to personal data in the possession of the organization, and it must correct, amend**,** or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

- *Enforcement***:** Data subjects must have access to some available and affordable independent mechanism that will investigate and resolve complaints and award damages where appropriate. If a company is subject to regulation the Federal Trade Commission (FTC) or the Department of Transportation (DOT), it satisfies this requirement because both agencies have pledged to enforce compliance with the Safe Harbor Principles.[122] Alternatively, a company must join a private sector privacy

[121] FAQ 1 - Sensitive Data, available at http://www.export.gov/safeharbor/FAQ1sensitivedataFINAL.htm.
[122] Both the FTC, *see* Letter to John Mogg, Director, DG XV, European Commission from Robert Pitofsky, FTC, July 14, 2000, available at http://www.export.gov/safeharbor/FTCLETTERFINAL.htm, and DOT, *see* Letter to John Mogg, Director, DG XV, European Commission from Samuel Podberesky, Assistant

program that includes an enforcement mechanism that meets the previous requirements. If, however, a company transfers human resources data from the EU to the US, it must agree to cooperate with EU data protection officials if a violation occurs.[123] This requirement ensures that European employees do not have to seek a remedy in the US for violation of the Principles.[124]

In addition to providing for an effective remedy, an organization must have procedures for verifying compliance with the Principles and for remedying problems arising out of failure to comply with the Principle, including sanctions which are sufficiently rigorous to ensure compliance by employees of the organization. A company is therefore obligated to audit its data processing policies or hire an independent third party to perform to audit.[125]

Finally, an organization that certifies that it will adhere to the Principles may be able to avoid compliance in three circumstances.[126] First, it can alter compliance as necessary to meet national security, public interest, or law enforcement requirements. Second, it can alter compliance to comply with conflicting statutes, regulations or case law, if it can demonstrate that its non-compliance is limited to the extent necessary to comply with a conflicting legal obligation. Third, an organization need not comply with the Principles if the processing of personal data qualifies for an exception or derogation under the Directive or member state laws, provided such exceptions or derogations are applied in comparable contexts.

Safe Harbor Implementation

There is evidence that some companies are ignoring the Safe Harbor Agreement and other companies have failed to implement all of its provisions. A Commission Staff Working paper adopted in 2002 found that a relatively few companies had become self-certified.[127] By the time of a 2004 staff report, there had been 400 self-certifications, which was still "lower" than the Commission initially had anticipated.[128] There are

---

General Counsel for Aviation Enforcement and Proceeding, DOT, July 14, 2000, available at http://www.export.gov/safeharbor/DOTLETTERFINAL.htm, indicated that they could prosecute a company under their jurisdiction for an "unfair or deceptive act or practice" if it failed to fulfill commitment to abide by the principles.

[123] FAQ 9 - Human Resources, available at http://www.export.gov/safeharbor/FAQ9HumanResFINAL.htm.

[124] Rehder & Collins, *supra* note __, at 148.

[125] FAQ 7 – Verification, available at http://www.export.gov/safeharbor/Faq7verifFINAL.htm.

[126] *Id.*

[127] Commission Staff Working Paper: The application of Commission Decision 20/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce**,** Feb. 13, 2002, SEC (2002) 196, at 5, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf.

[128] Commission Staff Working Paper: The Implementation of Commission Decision 20/2000/EC on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce**,** November 17, 2004, SEC (2004) 1323, at 5, 13, available at http://register.consilium.eu.int/pdf/en/04/st14/st14849.en04.pdf.

currently over 600 currently registered participants.[129] The 2004 report also reviewed the information privacy policies of companies which were self-certified and which had made their policies publicly available. This review indicated that many of the published policies did not conform to all of the Safe Harbor principles, which caused the authors of the report to conclude that there were compliance problems the EU must overcome.[130] In light of these compliance problems, the report was critical of the FTC for its lack of effort to ensure compliance with the principles.[131]

Despite these concerns, the Commission has indicated its intent to allow the Safe Harbor process to continue, although it made a number of recommendations for improvement.[132] Other voices are not as sanguine. Some data authorities and legislators believe the Safe Harbor process does not offer sufficient protection for personal data.[133] The Working Party also appears to be skeptical of significant aspects of the process.[134] Professor Reidenberg doubts the FTC has jurisdiction to enforce the provisions of the Safe Harbor Agreement in light of case law holding the agency does not have statutory authority to protect American business interests or foreign consumers.[135]

Because of the economic importance of data transfers to the US, the Commission appears to be proceeding cautiously despite the not insignificant problems with the safe harbor process. Nevertheless, the political situation may change. As Christopher Kuner has observed, if the safe harbor process "continues to gain companies and complaint resolution proceedings work well," the process is likely to remain "part of the data protection landscape," but if a "major scandal were to erupt involving the use of data by a safe harbor company, then political pressure in Europe to scuttle the safe harbor system might put its viability in jeopardy."[136]

Aviation Passenger Data

The Safe Harbor Agreement was based on the clause in Directive 95/46 that permits the transfer of data to a third country inadequate data protection if the controller furnishes adequate safeguards using contractual clauses or other means. Based on this clause, the US and the Commission have negotiated another agreement which addresses the transfer of airline passenger data from the EU to the US. The agreement was negotiated as a response to the Aviation and Transportation Security Act (ATSA),[137] which requires airlines to give the United States Bureau of Customs and Border Protection (CBP)

[129] **Verify this number**
[130] *Id*. at 8. This conclusion was based on a consultant's report that surveyed such policies. *See* Safe Harbor Implementation Study (April 19, 2004), at 13-14 , available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/safe-harbour-2004_en.pdf.
[131] 2004 Safe Harbor Working Paper, *supra* note __, at 10-11.
[132] *Id*. at 13-14.
[133] KUNER, *supra* note __, at 146.
[134] Art. 29 Working Party, Working Document on the Functioning of the Safe Harbor Agreement, July 2, 2002, available at http://www.datenschutz-berlin.de/doc/eu/gruppe29/wp62/wp62_en.pdf.
[135] Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 741 (2001).
[136] KUNER, *supra* note __, at 146.
[137] Aviation & Transportation Security Act of 2001, Pub. L. No. 107-71, 115 Stat. 597 (codified as amendment in scattered sections of 49 U.S.C.).

passenger name records for any aircraft leaving or entering the US.[138] This agreement, like the Safe Harbor agreement, did not come easily, and its legality is currently being challenged by the European Parliament and the Data Protection Supervisor.

The Commission negotiated the aviation agreement in order to head off the disruption of aviation between Europe and the United States. Airlines could not legally transmit passenger data to the CBP as ATSA required because the US did not qualify as a third country with adequate data protection laws. The US, however, threatened to search passengers arriving from Europe if the passenger data was not transmitted as legally required, which would have created extensive delays.[139] As a stop-gap measure, the Commission and CBP issued a joint statement in February 2003 that the American agency had given sufficient data protection guarantees that the transfer of passenger data to the US was temporarily lawful under the Directive.[140] A final agreement was reached in December 2003 and approved by the Commission.[141] The agreement limits what type of information an airline must transfer regarding a passenger, establishes a three and one-half year limit on storing such information, commits the Chief Privacy Officer of the Department of Homeland Security to reviewing complaints about the processing of data in an expedited fashion, and establishes yearly meetings between the CBP and the Commission to review how the US has implemented the agreement.[142]

Other EU institutions were active in opposing the aviation agreement, and the ECJ is now determining its legality. During the negotiations for a final agreement, the Article 29 Working Party expressed a number of reservations about the scope, nature, and us of the information that the US proposed to collect,[143] as did data privacy officials in the member states,[144] and the EU Parliament passed two resolutions criticizing the Commission's conduct of the negotiations and threatening to take the Commission to court.[145] The

---

[138] 49 U.S.C. §44909(c); see also 19 C.F.R. §122.49, 122.151 (implementing regulations). [**check this**]

[139] Bignami, *supra* n. __, at 863.

[140] European Commission / US Customs talk on Passenger Name Record (PNR) transmission, Joint Statement (Feb. 17/18, 2003), available at http://europa.eu.int/comm/external_relations/us/intro/pnr-joint03_1702.htm.

[141] Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, 2004 O.J. (L 235) 11, available at http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004D0535:EN:HTML.

[142] Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration, available at http://www.dhs.gov/interweb/assetlibrary/CBP-DHS_PNRUndertakings5-25-04.pdf.

[143] Opinion 4/2003 of the Working Party on the Level of Protection ensured in the U.S. for the Transfer of Passengers Data, 11070/03/EN, WP 78 (June 13, 2003), available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp78_en.pdf.

[144] *See* Arnulf S. Gubitz, *The U.S. Aviation and Transportation Security Act of 2001 in Conflict With the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need To Combat Terrorism?*, 39 NEW ENG. L. REV. 431, 465-66 (2005) (describing views of member state data protection officials).

[145] European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights (P5_TA(2003)0097) (March 13, 2003), available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/ce061/ce06120040310en03810384.pdf; European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights: state of negotiations with the USA (October

Parliament objected that the limitations on the use of personal data were overly broad, the US was permitted to collect information that was not related to protection against terrorism, the time limit on storing personal data was too long, and that the Chief Privacy Officer of the Department of Homeland Security did not have the necessary independence to enforce effectively the data protection rights of EU residents.[146] In December 2003, the Parliament approved a resolution condemning the Commission's decision to approve the agreement.[147] As noted earlier, the Commission is not bound by the vote because Parliament's powers are limited to determining whether the Commission had failed to follow proper procedures in negotiating and drafting the agreement. In April, 2004, the EU Parliament challenged the agreement in the ECJ.[148] The ECJ permitted European Data Supervisor to intervene in the law suit to support Parliament's position.[149] The Advocate General has recommended that ECJ find in favor of the Parliament's motion to annual the Commission's decision approving the transfer of passenger data.[150] A decision by the ECJ had not been made at the time this chapter was written.

Contract Clauses

The Safe Harbor and aviation agreements legalized data transfers to the US because these agreements furnish adequate privacy safeguards according to the Commission. Directive 95/46 also permits third country transfers if a data controller furnishes adequate safeguards through appropriate contractual clauses.[151] In 2001 and 2002, the Commission approved two sets of standard clauses that could be used to satisfy this exception. One applies to a "controller-to-controller" transfer or the transfer of personal data from a controller in the EU to a controller in a third country.[152] A company in the United States, for example, can use these contract provisions to qualify for the transfer of employment data from an EU-subsidiary to an American subsidiary. The other contract provisions apply to a "controller-to-processor" transfer or the transfer for data from a

---

9, 2003), 2004 O.J. (C 81 E) 105, available at http://www.epic.org/privacy/airtravel/profiling/epresolution.html.

[146] Bignami, *supra* note __, at 864.

[147] European Parliament resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection, (P5_TA-PROV(2004)0245) (March 31, 2004), available at http://www.cfp2004.org/program/materials/c14-pv2.html.

[148] Request for an Opinion submitted by the European Parliament under Article 300(6) of the EC Treaty, 2004 O.J. (C 118) 1, available at http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/c_118/c_11820040430en00010002.pdf.

[149] Order of the Court, European Parliament v. Council of the European Union, Case C-317/04 (March 17, 2005).

[150] PRESS RELEASE No 98/05, Opinion of the Advocate General in Cases C-317/04 and C-318/04 European Parliament v Council of the European Union and European Parliament v Commission of the European Communities, 22 November 2005, available at http://curia.eu.int/en/actu/communiques/cp05/aff/cp050098en.pdf.

[151] *See* note _ & accompanying text.

[152] Commission Decision 2001/497/EC, 2001 O.J. (L 181) 19, available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_181/l_18120010704en00190031.pdf.

controller in the EU to a processor of data in a third country.[153] An EU company, for example, can use these contract provisions to transfer data to a third country for outsourcing purposes. There are two different contract provisions because the Commission concluded controller-to-processor transfers did not require the same level of safeguards as controller to controller transfers.[154] The second type of transfer is more problematic because the original controller loses control of the personal data when it is transferred to another controller.[155] Although the Commission intended that these contract provisions would facilitate the transfer of data, the controller-to-controller provisions were criticized for being too inflexible and burdensome to be commercially realistic.[156] In 2005, the Commission responded by approving standard controller-to-controller contract clauses proposed by seven business associations.[157]

The standard contract provisions expressly authorize data subjects to enforce their rights as third-party beneficiaries for specific breaches of the contract clauses.[158] This gives employees the capacity to obtain compensation as a result of a breach of a contract clause by either the data exporter or importer.[159]

Codes of Conduct

Finally, although Directive 95/46 specifically authorizes the use contract provisions, it also contemplates that there may be other methods of providing the necessary protection.[160] Using this authority, national data authorities can approve third country transfers of personal data if a company adopts an adequate code of conduct. According to the Article 29 Working Party, a code of conduct consists of "binding corporate rules for international data transfers" or "legally enforceable corporate rules for international data transfers."[161] At a minimum, a code must be approved by a company's board of directors, or a comparable body of the group's parent company, and be binding on all company employees.[162] Since a Code of Conduct only applies to transfers of data to members within the same corporate group, it must forbid the transfer of personal data to non-EU based third parties because they are not subject to the provisions of the Code or to the EU privacy legislation. To transfer data to such third parties a company must base

[153] Commission Decision 2002/16/EC, 2002 O.J. (L 6) 52, available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_006/l_00620020110en00520062.pdf
[154] Rehder & Collins, *supra* note __, at 140.
[155] *Id*.
[156] See KUNER, *supra* note __, at 150-52; Huie, Laribee & Hogan, *supra* n. __, at 451.
[157] Commission Decision 2004/915/EC, 2004 O.J. (L 385) 74, available at http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00740084.pdf .
[158] Commission Decision 2001/497/EC, *supra* n. __, at Clause 3; Commission Decision 2002/16/EC, *supra* n. __, at Clause 3.
[159] Rehder & Collins, *supra* note __, at 141.
[160] *See* note __ & accompanying text.
[161] Article 29-Data Protection Working Document: Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfer, June 3, 2003, 11639/02/EN WP 74, at 8, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf.
[162] Rehder & Collins, *supra* n. __, at 152.

the transfer on other approved measures, such as the Safe Harbor agreement or EU-approved standard contract clauses.[163]

In addition to making the Code binding, data subjects must have a remedy under the Code for its breach.[164] A company can do this by making data subjects a third-party beneficiary of the Code,[165] as in standard contract remedies.[166] Whatever the source of the remedy, it should at least match the rights set forth in the Controller-to-Controller standard contractual clauses.[167]

Codes of conduct are subject to the approval of the data protection authority in the member state in which the transfer of data originates.[168] Moreover, the approval of one member state is not binding on other member states,[169] although the EU is seeking to promote the cooperation of various member state data authorities.[170]

REGULATION 45/2001

Directive 95/46 establishes the requirements and framework for the protection of personal data in the member states. Regulation 45/2001[171] serves the same function for personal data in the possession of EU institutions. While the US has no counterpart to Directive 95/46, the Privacy Act[172] in the United States operates much like Regulation 45/2001. Regulation 45/2001, however, provides additional protections and remedies that are not available under the Privacy Act, which reflects the greater importance attached to protecting privacy in Europe.

The protections afford by Regulation 45/2001 closely resemble those provided in the Directive 95/46. As with Directive 95/46, there have been conflicts between data protection and data access when the disclosure of personal data is involved. This section describes the scope of Directive 95/46, the regulatory institutions used to implement it, and the tension between the data protection regulation and the data access regulation.

Requirements

Like Directive 95/46, Regulation 45/2001 applies to the "processing" of "personal data" by a "controller." In this context, a "controller" is any "Community institution or body, the Directorate-General, the unit or any other organizational entity which alone or jointly with others determines the purposes and means of the processing of personal data …."[173]

---

[163] Rehder & Collins, *supra* n. __, at 152.
[164] Working Party On Binding Corporate Rules, *supra* n. __, at 11.
[165] Rehder & Collins, *supra* n. __, at 153.
[166] *See* note __ & accompanying text.
[167] Working Party On Binding Corporate Rules, *supra* n. __, at 12.
[168] *See* note __ & accompanying text.
[169] Rehder & Collins, *supra* n. __, at 155.
[170] Working Party On Binding Corporate Rules, *supra* n. __, at 20.
[171] Commission Regulation 45/2001, 2000 O.J. (L8) 1.
[172] 5 U.S.C. §552a.
[173] Commission Regulation 45/2001, *supra* note __, at art. 2(d).

Both "personal data" [174] and "processing" [175] are defined in the same way as they are in Directive 95/46. Regulation 45/2001 prohibits an EU institution from "processing" any "personal data" except as necessary to carry out administrative obligations, requires it to ensure the accuracy and completeness of such data, and prohibits it from maintaining personal data any longer than it is needed for a legitimate purpose.[176] Furthermore, the regulation prohibits the processing personal data without the "unambiguous" consent of an individual or unless the processing fits within a list of other exceptions.[177] If, however, the processing concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life, the controller must have the "explicit" consent of the individual or the processing must satisfy three other narrow exceptions.[178] The reader will recall that in order to obtain "explicit" consent, a controller must use an "opt-in" method of obtaining consent.[179] EU institutions are prohibited from transferring data to other recipients which are not subject to Directive 95/46 or which do not provide an adequate level of protection,[180] thereby giving the Regulation extra-territorial application. Some limited types of disclosures, however, are exempted from some of the prior requirements.[181]

Remedies

In order to enforce the previous requirements, Regulation 45/2001 establishes a system of remedies for data subjects for the illegal acquisition, maintenance, or processing of personal data. First, each institution has an affirmative obligation to provide a data subject with detailed information about information collected about that individual.[182] Second, an individual has the right to block the processing of information in certain circumstances,[183] such as during the period when there is an unresolved dispute over the accuracy of the data, and to have information erased when information has been obtained or maintained in violation of the Regulation.[184] Third, the European Court of Justice has jurisdiction to hear all disputes relating to compliance including claims for damages.[185] Finally, an individual can bring a complaint to the European Data Supervisor, which is discussed in the following section.

Regulatory Institutions

---

[174] *Id*. at art. 2(a); s*ee* note _ & accompanying text (definition of "personal data" in Directive 45/2001).
[175] Commission Regulation 45/2001, *supra* note __, at art 2; s*ee* note _ & accompanying text (definition of "processing" in Directive 45/2001).
[176] Commission Regulation 45/2001, *supra* note __, at art. 4-6.
[177] *Id*. at art. 5.
[178] *Id*. at art 10.
[179] See *infra* notes ___ & accompanying text (discussing the distinction between "unambiguous" and "explicit" consent").
[180] *Id*. at art 9.
[181] *Id*. at art 20.
[182] *Id*. at art 11-12.
[183] Commission Regulation 45/2001, *supra* note __, at art 15.
[184] *Id*. at art 16.
[185] *Id*. at art. 32.

To help implement the previous protections, Regulation 45/2001 establishes two institutions. First, the EU has established an administrative position, the European Data Protection Supervisor, with responsibility for compliance with the regulation. The Supervisor is appointed by the European Parliament and the Council for a term of five years from a list of candidates drawn up by the Commission.[186] The duties of the Supervisor include monitoring compliance with the Regulation, giving an opinion on the legality of processing operations likely to present specific risks to the rights and freedoms of data subjects, hearing and investigating complaints, and offer general advice about the implementation of the Regulation.[187] The Supervisor has the power to order the rectification, blocking, erasure, or destruction of data processed in breach of the regulation, impose temporary or permanent bans on the processing of specific information, refers disputes to the European Court of Justice, and intervene in disputes filed by other persons or entities in the ECJ.[188]

A data subject can file a complaint with the Data Protection Supervisor without prejudicing any right to a judicial remedy.[189] As noted, the Supervisor has the authority to order the rectification, blocking, erasure, or destruction of data that has been processed in violation of the Regulation. The European Court of Justice has jurisdiction to hear all disputes relating to compliance, including claims for damages.[190]

Second, each community institution must appoint a "Data Protection Officer" who has the responsibility of ensuring the institution's compliance with the regulation.[191] Although the officer is appointed by each institution for a term of two to five years, the person may be dismissed only with the permission of the Supervisor and only if the person "no longer fulfills the conditions required for the performance or his or her duties."[192] An institution is prohibited from assigning other duties to an Officer if the assignment would result in a conflict of interest with the Officer's implementation of the Regulation 45/2001.[193] The institution must also notify the Officer prior to the processing of personal data and give detailed information about the planned operation.[194] It must also consult with the Officer prior to the use of information that presents specific risks to the data subject by virtue of the nature, scope, or purpose of information processing.[195]

TRANSPARENCY

The EU has established a significant regulatory regime to protect personal data in the possession of EU entities which matches the level of protection that the member states must provide according to the privacy directives. As with Directive 95/46, the broad

[186] *Id*. at art. 41-42.
[187] *Id*. at art 46.
[188] *Id*. at art. 47.
[189] *Id*.
[190] *See* notes _ & accompanying text.
[191] Commission Regulation 45/2001, *supra* note __, at art. 24.
[192] *Id*. at art. 24.
[193] *Id*. at 24.
[194] Commission Regulation 45/2001, *supra* note __, at art 25.
[195] *Id*. at art 27.

protection of privacy must be reconciled with transparency requirements. This section considers the relationship of the data protection and data access regulations, and the impact of this relationship on governmental transparency.

Regulation 45/2001 permits the disclosure of personal data as "necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities *or other legal instruments adopted on the basis thereof* …."[196] If, therefore, the data access regulation requires the disclosure of personal data, Regulation 45/2001 permits such a disclosure. The data access regulation requires the disclosure of all data unless an exemption applies, and there is an exemption for to protect personal privacy and integrity. Article 4.1 of the access regulation prohibits disclosure if it "would undermine the protection of … (b) privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data."[197]

There are two noteworthy aspects of Article 4.1. First, the exception uses compulsory and absolute language. According to the exception, "institutions *shall* refuse access to a document where disclosure would undermine the protection of … the privacy and the integrity of the individual."[198] Moreover, in contrast with other disclosure exceptions, the privacy exception is not subject to an overriding pubic interest in disclosure.[199] This absence of this qualification and the absolute nature of the language both suggest that information falling within the scope of the privacy exception must be protected, and the right to protection is not to be balanced against the public's interest in seeing the information.[200]

These characteristics distinguishes Article 4.1 from the privacy exception of the Freedom of Information Act (FOIA), which permits the disclosure of personal information unless it would "constitute a clearly unwarranted invasion of personal privacy."[201] Understandably, courts in the United States regard this language as favoring disclosure over the protection of privacy.[202]

Second, while Article 4.1 protects personal privacy, the scope of protection is not clear. Some early decisions of the Commission interpret Article 4.1 as protecting personal data anytime such data would be protected by Regulation 45/2001. The Ombudsman has offered a narrower interpretation of Article 4.1, which has been endorsed by the EU

---

[196] Commission Regulation 45/2001, art 5(a), 2000 O.J. (L8) 1, 5 (emphasis added)
[197] Commission Regulation 1049/2001, art. 4, 2001 O.J. (L. 145), 43.
[198] *Id*. (emphasis added).
[199] For example, another exception provides that institutions "shall refuse access to a document where disclosure would undermine the protection of commercial interests of a natural or legal person, including intellectual property, ... *unless there is an overriding public interest in disclosure.*" *Id*. at art. 4.1.
[200] *See* European Data Protection Supervisor, Public Access to Documents and Data Protection §2.4.3 (July 2005), available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf.
[201] 5 U.S.C. 552(6).
[202] *See, e.g.*, Kurzon v. HHS, 649 F.2d 65, 67 (1st Cir. 1981) (the case in which "the calculus unequivocally supports withholding is rare because Congress has weighted the balance so heavily in favor of disclosure ….")

Parliament. The Data Protection Supervisor, however, disagrees with the Ombudsman's position based on case law in the ECJ.

Commission Decisions

Since Article 4.1 prohibits the disclosure of data "in accordance with Community legislation regarding the protection of personal data," the Commission early on interpreted it to forbid disclosure unless disclosure is permitted by the privacy regulation itself. Under this interpretation, personal data cannot be disclosed under the data access regulation unless disclosure is permitted according to one of the exceptions found in Regulation 45/2001. If none of those exceptions apply, disclosure would be forbidden under the data access regulation as well as the privacy regulation.

The Commission took this position, for example, after a German beer company, Bavarian Lager, filed a complaint with the Commission alleging the United Kingdom was discriminating against foreign beers, there was a meeting between the Commission, UK trade authorities, and a trade association to discuss the issue. The beer company sought access to the names of the persons who attended the meeting, which the Commission denied on the grounds that Directive 45//2001 prevented it from disclosing the identities of the persons concerned without their express permission.[203] In another example, a newspaper applied for public access under Regulation 1049/2001 to see a public register of approvals given for external activities of Commission officials. The Commission supplied the register, but deleted all the names of the officials concerned, contending that the data protection regulation gives these persons the right to remain anonymous.[204]

Ombudsman's Interpretation

The Ombudsman objected to the Commission decisions as constituting a substantial roadblock to transparency. He proposed that Article 4.1 of the access regulation only protects information that relates to that relate to private and family concerns and not to information that relates to persons acting in a public capacity. The Ombudsman based this interpretation on Article 8.1 of the Charter of Fundamental Rights of the European Union,[205] which reads: "Everyone has the right to respect for his or her private and family life, home, and communications."[206] Accordingly, the Ombudsman argues "the right to privacy with respect to the processing of personal data under the Data Protection Directive does not require the Commission to treat as secret views or information which

[203] Special Report from the European Ombudsman to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH (Nov. 23, 2000), at 1-4, available at http://www.euro-ombudsman.eu.int/special/pdf/en/980713.pdf.
[204] The European Ombudsman Letters and Notes, The Misuse of Data Protection Rules in the European Union, available at http://www.euro-ombudsman.eu.int/letters/en/20020925-1.htm.
[205] Special Report from the European Ombudsman to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH (Nov. 23, 2000), available at http://www.euro-ombudsman.eu.int/special/pdf/en/980713.pdf.
[206] European Convention on Human Rights, art. 8.1, available at http://www.hri.org/docs/ECHR50.html#C.Art8

have been submitted to it concerning the exercise of its functions, nor the names of the persons who submitted the views or information."[207]

In December 2001, the European Parliament adopted the Ombudsman's position. Parliament indicated that the "aim of data protection is primarily to protect the private life and sensitive information," and data protection was therefore inapplicable to persons "acting in a public capacity, while they are taking part in public decision making on their own initiative or while they try to influence such decision making."[208]

Data Protection Supervisor

The European Data Protection Supervisor has sought to clarify the scope of the privacy exception to the data access regulation in light of the Ombudsman's recommendation. The Supervisor believes that some types of personal information relating that arise in a governmental or business context may be protected by the language in the data access regulation.[209] He bases this interpretation on a decision of the ECJ involving Directive 95/46.

In *Österreichischer Rundfunk and Others* case,[210] the ECJ considered the application of the data protection directive to a German law which required a large number of governmental bodies to disclose publicly the salaries and pensions of officials earning more than a certain amount of money. As mentioned earlier,[211] the Court found that the salary information was "personal data" within the scope of Directive 95/46, although the court also held that the Directive permitted the publication of the data if the national court determined it was necessary and appropriate for its intended purposes. The ECJ found that the compensation information was "personal data" within the scope of the Directive 95/46 on the basis of a decision the European Court of Human Rights.

In *Amann v. Switzerland*,[212] the European Court of Human Rights interpreted Article 8 of the Convention of Human Rights. Article 8.1 of the Convention, as noted earlier, establishes a person has "the right to respect for his private and family life, his home and his correspondence."[213] Article 8.2 forbids "interference by a public authority with the exercise of this right" except when it is necessary for the interests of national security, public safety and similar justifications, and except as it is "in accordance with the law."[214] *Amann* held the government of Switzerland had violated Article 8 when it intercepted a

[207] Special Report from the European Ombudsman, *supra* note __, at ¶ 2.7.
[208] Parliament's resolution supporting Ombudsman on access to public information overriding the secrecy of personal data in EU institutions' hands (Dec. 12, 2001), available at http://www.publicinfo.net/forprint.php?allvars=18020412875500000020 2001-12-140i
[209] European Data Protection Supervisor, Public Access to Documents and Data Protection (July 2005), at §4.3.3, available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf.
[210] Case C-465/00, Rechnungshof v. Osterreichischer Rundfunk and Others, 2003 ECR I-4989.
[211] *See* notes _ & accompanying text.
[212] (2000) 30 E.H.R.R. 843.
[213] European Convention on Human Rights, art. 8.1, available at http://www.hri.org/docs/ECHR50.html#C.Art8.
[214] *Id*. at art. 8.2

phone call received by a government employee and made a record of the call because the action violated the employee's right to privacy and it was not authorized by law. Concerning the first conclusion, the Court noted:

> The term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature.[215]

.

In light of *Amann*, the Supervisor recommends that data relating to a person's business or governmental capacity may be protected by the privacy exception of the data access regulation. Although he acknowledges that the mere fact that a public record contains personal data does not mean privacy is involved,[216] he also maintains that disclosure of certain types of information in public records do involve a person's privacy. Specifically, personal data falls within the scope of the privacy exception of the public access regulation if disclosure involves the sensitive data, embarrassing data, data that reflects on a person's honor and reputation, data that places a person in a false light, or personal information which a person normally treats as confidential.[217] Moreover, because of proportionality, an institution can only withhold those portions of the document that undermine the privacy interest. [218]

CONCLUSION

The Europeans take personal privacy seriously. There is an elaborate and extensive regulatory framework that protects personal privacy in the EU, and the EU has sought to protect the privacy of its residents when personal data is transferred to countries outside of the EU. Although the United States has legislation protecting personal privacy in some sectors, there is no comparable overall regulatory framework in this country.

The EU has directed the member states to regulate personal data in the possession of private and public entities in Directive 95/46, which establishes a general regulatory framework, and Directive 2002/58, which applies to personal data in the electronic communications sector. Member states have established data protection authorities in response to the Directive to implement protective regulation. Regulation 45/2001 protects personal data in the possession of EU institutions. While it is similar to the Privacy Act in the United States, it provides more protection and remedies. The regulation established the EU Data Protection Supervisor to ensure compliance with the regulation.

The protection of personal data in the EU has two ramifications for Americans. For persons doing business in the EU, they are subject to privacy regulation in the member

---

[215] *Amann*, *supra* note __, at 845, ¶2(a).
[216] European Data Protection Supervisor, *supra* note __, at §4.3.1.
[217] *Id*. at §4.3.3.
[218] *Id*. at §4.2.2-4.3.3.

states. Moreover, since the EU gives extra-territorial application to Directive 95/46, the transmission of personal information from the EU to the US is regulated.

The EU's efforts to protect personal data have been impacted by three developments. First, since member states have some discretion under Directive 95/46 to develop their own implementation and enforcement policies, they have diverged in their implementation of Directive 95/46. This development has created problems for effective implementation and the maintenance of an integrated market. While there are efforts by the EU to harmonize the approaches used in the member states, these efforts confront the reality that member states have somewhat different policy views concerning the details of how personal privacy is protected.

The protection of personal data has also been impacted by data access requirements. Member states and EU institutions are in the process of reconciling the protection of personal data with data access mandates. This conflict is more of a problem in the EU than it is in the US because of the stronger commitment to protecting personal data. In the US, conflicts between data protection and data access are generally resolved in favor of access. In the EU, however, both data protection and government transparency are considered of fundamental importance, and the reconciliation of these goals is therefore more difficult.

Finally, the EU's efforts to protect personal data when it is transmitted outside of the EU have created conflicts with maintaining and enhancing international trade. The EU does not permit the transfer of personal data unless the recipient country offers an adequate level of protection for such data, or unless there are other arrangements in place that will offer a level of protection comparable to that in the EU. Since the EU does not regard the United States as meeting the first option, the EU and the US have negotiated two controversial agreements that allow data transfers under the second option. Critics, including a majority of the EU Parliament, believe that the Commission has signed the agreements despite the fact that they offer inadequate protection in order to maintain trade with the US. The tension between interest in facilitating trade and protecting personal data is not likely to abate as long as commercial and governmental interests in the US and other non-EU countries seek to avoid providing comparable privacy protections in order to reduce their costs.

Despite these difficulties, Europeans have a level of protection for personal privacy that is considerably greater than in the United States. This result reflects differences in the historical, cultural and political characteristics of the EU and the US. It also means that the EU is not likely to reduce significantly the regulatory protections that it has established.