__. 0 DATA PROTECTION

In the EU, data protection, as well as data access, is considered as a fundamental right. Reflecting this significance, the EU has broad and extensive protections for personal data. Both EU institutions and the member states are the subject of data protection legislation in the EU. Regulation 45/2001 protects the privacy rights of individuals concerning data in the possession of governmental institutions at the level of the EU. Directive 95/46 requires member states to establish regulatory regimes that safeguard privacy rights concerning data in the possession of member state institutions and private entities. Data protection regulation is more extensive in the EU than comparable legislation in the United States.

The status of data protection as a fundamental right reflects a long and 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.[1] 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.

The importance of privacy rights in the EU has created a tension between data access and data protection. This section of the chapter examines data protection legislation in the EU and the conflict between data protection and data access legislation.

_.1 Regulation 45/2001

The regulatory process established by Regulation 45/2001 is similar to the one established by the Privacy Act in the United States. EU regulation, however, gives more protection to personal data, and is overseen by an independent agency, the European Data Protection Supervisor.

_.11 Regulatory Process

Regulation 45/2001 applies to the "processing" of "personal data" by a "controller."

- 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 ...."[2]
- "Personal data" is "any information relating to an identified or identifiable natural person," known as a "data subject." Information "relates" to a data

[1] ECHR art. 8(1).
[2] Commission Regulation 45/2001, art. 2(d), 2000 O.J. (L8) 1, 4.

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."[3]

- 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."[4]

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.[5] Furthermore, the regulation prohibits the disclosure or dissemination of personal data without the "unambiguous" consent of an individual subject to a list of some exceptions.[6] When information is disclosed or disseminated, the institution must maintain records concerning the nature of the disclosure, subject to some exceptions.[7] Some limited types of disclosures, however, are exempted from some of the prior requirements.[8]

This regulatory framework is similar to the regulatory process created by the Privacy Act in the United States. The Privacy Act protects personal information in "records" maintained by agencies, and a "record" is any information "about an individual that is maintained by an agency …. and that contains [an individual's] name, or the identifying number, symbol, or other identifying particular assigned to the individual …."[9] It establishes similar limitations on the acquisition and maintenance of personal data,[10] and it likewise requires a person's consent for the dissemination of personal information, subject to exceptions.[11] Finally, the Privacy Act also exempts some type of data from the requirements of the Act.[12]

Both the Privacy Act and Regulation 45/2001 establish a procedure for individuals to seek the correction of erroneous information. The Privacy Act requires agencies to give individuals access to their records, to permit them to request amendments of those records and to appeal a decision not to make a correction, and to notify any recipients of personal information if there is a pending and unresolved dispute concerning it.[13]

---

[3] Commission Regulation 45/2001, art. 2(a), 2000 O.J. (L8) 1, 4.
[4] Commission Regulation 45/2001, art 2, 2000 O.J. (L8) 1, 4.
[5] Commission Regulation 45/2001, arts. 4-6, 2000 O.J. (L8) 1, 5-6.
[6] Commission Regulation 45/2001, art 5, 2000 O.J. (L8) 1, 5.
[7] Commission Regulation 45/2001, art 12-13, 2000 O.J. (L8) 1, 9.
[8] Commission Regulation 45/2001, art 20, 2000 O.J. (L8) 1, 11.
[9] 5 U.S.C. §552a(a)(4).
[10] 5 U.S.C. §552a(e).
[11] 5 U.S.C. §552a(b).
[12] 5 U.S.C. §552a(k).
[13] 5 U.S.C. §552a(d).

Regulation 45/2001 provides a similar protections and some additional ones. An individual has the right to block the use of information in certain circumstances,[14] 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.[15]

The EU regulation is more protective of persona data than the Privacy Act in several additional ways.

- Institutions are forbidden from processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and concerning health of sex life except with the "explicit" consent of the individual or if three other narrow exceptions apply.[16]
- An institution must provide a data subject with detailed information about information collected about that individual.[17] The Privacy Act permits individuals to obtain similar information, but only if they request it.[18]
- An institution must notify the Data Protection Officer prior to the use of personal information and give detailed information about the planned operation.[19] An institution must also consult with the Data Protection 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.[20]
- A data subject can file a complaint with the Data Protection Supervisor without prejudicing any right to a judicial remedy.[21] As explained below, the Supervisor has the authority to order the rectification, blocking, erasure, or destruction of data that has been processed in violation of the Regulation.
- US courts may award damages under the Privacy Act only in cases of intentional and willful violations, although a plaintiff can recover attorney's fees if the person "substantially prevails" in the litigation.[22] Regulation 45/2001 authorizes the courts to award damages without any similar limitation.[23]

__.12 Institutional Structure

Regulation 45/2001 and the Privacy rely on a similar institutional structure. The EU legislation applies to all "community institutions,"[24] and the European Court of Justice has jurisdiction to hear all disputes relating to compliance including claims for

[14] Commission Regulation 45/2001, art 15, 2000 O.J. (L8) 1, 10.
[15] Commission Regulation 45/2001, art 16, 2000 O.J. (L8) 1, 11.
[16] Commission Regulation 45/2001, art 10, 2000 O.J. (L8) 1, 8.
[17] Commission Regulation 45/2001, arts 11-12, 2000 O.J. (L8) 1, 9-10.
[18] 5 U.S.C. §552a(e)3).
[19] Commission Regulation 45/2001, art 25, 2000 O.J. (L8) 1, 14.
[20] Commission Regulation 45/2001, art 27, 2000 O.J. (L8) 1, 15.
[21] *Id*.
[22] 5 U.S.C. 552a(g).
[23] Commission Regulation 45/2001, art 32, 2000 O.J. (L8) 1, 16.
[24] Commission Regulation 45/2001, art. 2, 2000 O.J. (L8) 1, 4.

damages.[25] Similarly, the Privacy Act applies to all federal agencies,[26] and it authorizes the federal courts to grant injunctive relief for violations of the Act and, as noted above, to award damages for willful or intentional violations.[27]

Besides these provisions, Regulation 45/2001 requires each community institution to appoint a "Date Protection Officer" who has the responsibility of ensuring the institution's compliance with the regulation.[28] 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."[29] 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.[30]

The European Data Protection 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.[31] 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.[32] 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.[33]

_.2 Directive 95/46

Directive 95/46[34] establishes the obligation of the EU member states 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. A second directive, 58/2002[35], addresses the processing of personal data in the electronic communications sector. While the communications sector is subject to the first directive, the second directive reflects later developments in markets and technology for electronic communications services, such as the Internet.

The United States has no similar overarching legislation. Instead, Congress has required the protection of specific types of information in the possession of state or private

[25] Commission Regulation 45/2001, art. 32, 2000 O.J. (L8) 1, 16.
[26] 5 U.S.C. §552a(a)(1).
[27] *Id*. §552a(g).
[28] Commission Regulation 45/2001, art. 24, 2000 O.J. (L8) 1, 13.
[29] Commission Regulation 45/2001, art. 24, 2000 O.J. (L8) 1, 13.
[30] Commission Regulation 45/2001, art. 24, 2000 O.J. (L8) 1, 13.
[31] Commission Regulation 45/2001, arts. 41-42, 2000 O.J. (L8) 1, 18
[32] Commission Regulation 45/2001, art 46, 2000 O.J. (L8) 1, 20.
[33] Commission Regulation 45/2001, arts. 47, 2000 O.J. (L8) 1, 47.
[34] Council Directive 95/46, 1995 O.J. (L 281) 31.
[35] Council Directive 2002/58/EC, 2002 O.J. (L201), 37.

entities, such as education records,[36] consumer credit reports,[37] bank records,[38] cable company records,[39] health care provider records,[40] driver license information,[41] and information collected by web sites from children under the age of 18.[42] Thus, while the EU directive applies to all governmental institutions and private entities which process personal data, only some state agencies and commercial sectors in the United States are regulated.

__.21 Regulatory Process

Directive 95/96, which predates Regulation 45/2001, uses the same regulatory framework. It applies to the "processing" of "personal data" by "controllers," and the first two terms have the same definition as they have in Regulation 45/2001.[43] 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 …",[44] which obligates member states to regulate the possession of personal data in the possession of both government and private entities.

Directive 95/96 requires legislation that prohibits controllers from acquiring "personal data" except for "specified, explicit and legitimate purposes" and from processing information in any way incompatible with those purposes.[45] Such legislation must also obligate controllers to ensure the accuracy and completeness of such records, and prohibit the maintenance of personal data after it is no longer needed for a legitimate purpose.[46] A country must also require controllers to provide data subjects with detailed information about what personal data they have about an individual,[47] and with the right to see such data, to rectify errors or erase or block erroneous information,[48] to seek judicial review of the breach of any rights, and to receive compensation for any damages.[49]

A member country law must also prohibit the disclosure or dissemination of personal data without the "unambiguous" consent of an individual subject to a list of some exceptions,[50] and it must forbid the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and

[36] Family Education Rights and Privacy Act (1974) (codified at 20 U.S.C. §1232g).
[37] Fair Credit Reporting Act (1970) (codified at 15 U.S.C. §1681 et. seq.).
[38] Right to Financial Privacy Act (1978) (codified at 12 U.S.C. 3401 et. seq.).
[39] Cable Communications Policy Act (1984) (codified at 47 U.S.C. §551 et. seq.).
[40] Health Insurance Portability and Accountability Act (2002) (codified at 42 U.S.C. §210).
[41] Drivers Privacy Protection Act (1994) (codified at 18 U.S.C. § 2721 et. seq.).
[42] Children's On-Line Privacy Protection Act (1999)(codified at 8 U.S.C. §1301).
[43] Council Directive 95/46, art. 2(a)-(b), 1995 O.J. (L 281) 31, 38.
[44] Council Directive 95/46, art. 2(d), 1995 O.J. (L 281) 31, 38.
[45] Council Directive 95/46, art. 6, 1995 O.J. (L 281) 31, 40.
[46] Council Directive 95/46, art. 6, 1995 O.J. (L 281) 31, 40.
[47] Council Directive 95/46, art. 10-11, 1995 O.J. (L 281) 31, 41-42..
[48] Council Directive 95/46, art. 12, 1995 O.J. (L 281) 31, 42.
[49] Council Directive 95/46, art. 22-23, 1995 O.J. (L 281) 31, 45.
[50] Council Directive 95/46, art. 7, 1995 O.J. (L 281) 31, 40.

concerning health of sex life except with the "explicit" consent of the individual unless one of several narrow exceptions apply.[51]

Finally, but hardly least of all, the Directive requires member states to impose an obligation on controllers to ensure the security of personal data. Specifically, member states must "provide that the controller must implement appropriate technical and organizational measures to protect personal data against unlawful destruction or accidental loss, alteration, [and] unauthorized disclosure or access …."[52] The Directive on privacy in electronic communications extends this requirement. A member state must obligate controllers to "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]."[53] In addition, member state law must require controllers to notify subscribers of the extent to which the risk of unauthorized disclosure is not eliminated by the measures taken by the controller.[54]

__.22 Regulatory Institutions

Besides specifying the nature of the regulatory process that a member state must establish, the Directive establishes requirements concerning the regulatory institutions used to implement the Directive. In general, countries must adopt "suitable measures to ensure full implementation" of the Directive and to establish "suitable sanctions" for infringement of data protection legislation.[55]

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.[56] Second, as noted above, 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.[57] Finally, the Directive also establishes an advisory "Working Party on the Protection of Individuals With Regard to the Processing of Data."[58] The 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.

__.23 Application to the United States

Directive 95/96 has extra-territorial application because it forbids the transfer of personal data to third countries that do not have "adequate" data protection regulations,[59] subject

[51] Council Directive 95/46, art. 8, 1995 O.J. (L 281) 31, 40.
[52] Council Directive 95/46, art. 17, 1995 O.J. (L 281) 31, 43.
[53] Council Directive 2002/58/EC, art. 4, 2002 O.J. (L201), 37, 43.
[54] *Id*.
[55] Council Directive 2002/58/EC, art. 24, 2002 O.J. (L201), 37, 45
[56] Council Directive 95/46, art. 28, 1995 O.J. (L 281) 31, 47.
[57] Council Directive 95/46, art. 22-23, 1995 O.J. (L 281) 31, 45.
[58] Council Directive 95/46, art. 28, 1995 O.J. (L 281) 31, 47
[59] Council Directive 95/46, art. 25, 1995 O.J. (L 281) 31, 45.

to some exceptions.[60] After the Directive was enacted, the EU threatened to ban the transfer of personal data to the US because American laws protecting data privacy did not offer data subjects sufficient protection. The US Department of Commerce, however, found a way to protect American companies if the volunteer to provide heightened protection for personal data obtain from the EU.

The Directive, as noted, provides some exceptions to the prohibition of transmitting personal data to countries without inadequate data protection. The Department was able to take advantage of one of these exceptions. It provides a controller can transfer personal data to a country with inadequate protections if the controller "adduces" that "adequate safeguards" exist with respect to the protection of the privacy from "appropriate contractual clauses."[61] Furthermore, the Commission has the authority to determine that "certain standard contract clauses offer sufficient safeguards" to satisfy the previous exception.[62]

To qualify for the previous exception the Department developed a set of standard form contract provisions known as the "Safe Harbor" principles.[63] In July, 2000, the Commission ruled in the principles offered sufficient safeguards to qualify as an exception to any general ban on transferring personal data to the United States.[64] In December, 2000, the European Parliament made it necessary for US firms to abide by the Safe Harbor principles in order to receive personal data from the EU. The Parliament ruled that US law did not offer an adequate level of protection for personal data,[65] which activated a general ban on the transfer of such data. As a result, any data exchange between the EU and the US is prohibited unless it is pursuant to the Safe Harbor principles or other contractual arrangements that satisfy the Directive.

The Safe Harbor program is completely voluntary, but once a company elects to participate, adherence to the Safe Harbor principles becomes mandatory. In order to participate, a company must register with the Department of Commerce, providing a description of the company's existing privacy policies and of the policies that will be apply concerning personal data received from Europe. To ensure compliance, a company may join a private enforcement program, develop its own enforcement program, or self-certify that its preexisting privacy standards are in place and comply with the Safe Harbor principles.

---

[60] Council Directive 95/46, art. 26, 1995 O.J. (L 281) 31, 46.
[61] Council Directive 95/46, art. 26(2), 1995 O.J. (L 281) 31, 46
[62] Council Directive 95/46, art. 26(4), 1995 O.J. (L 281) 31, 46
[63] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (2000).
[64] Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce - O. J. L 215/7 of 25.8.2000.
[65] Elizabeth De Bony, *EU Rejects U.S. Data Privacy Protections As Inadequate* (July 7, 2000), available at http://archives.cnn.com/2000/TECH/computing/07/07/safe.harbor.idg/.

Organizations and participating companies must comply with a number of requirements that are similar to the mandates in Directive 95/96:

- The use of personal data must be relevant to the purpose for which it was collected, and companies must notify private individuals of the manner by which personal information is collected and used.
- Regarding any transfer of personal data to a third party, the third party must subscribe to the safe harbor principles and contract for the same level of privacy protection. Moreover, companies must permit individuals to "opt out" regarding the disclosure of personal data to a third party. If a company wishes to transfer 'sensitive" personal data to a third party, it must employ an "opt in" provision which obtains the "express" consent of the data subject for the transfer.
- Individuals must be given access to their personal data and the opportunity to amend it, subject to limited exceptions.
- Companies must take reasonable precautions to protect personal information.
- A company must have mechanisms to assure assuring compliance with the Safe Harbor principles, provide recourse for individuals affected by non-compliance, and administer sanctions to its employees severe enough to ensure future compliance.

The Principles anticipate that Federal Trade Commission or other federal agencies will enforce a company's promise to abide by the Principles. A company subject to the Federal Trade Commission Act, for example, may be liable for an "unfair trade practice" if it agrees to abide by the principles and fails to do so. Persistent failure to comply with Safe Harbor principles will result in exclusion from the safe harbor program and its accompanying benefits. The Principles also anticipate the EU citizens may file tort or contract actions in the US courts arising from a failure to abide by the Principles.

__.03 Impact on Transparency

The EU has established two significant regulatory regimes to protect personal data in the possession of governmental and private entities. These regimes reflect the understanding in the EU that there is a fundamental right to personal privacy. There is, however, also a fundamental right to governmental transparency. When individuals seek governmental records containing personal data, a clash between these two fundamental rights cannot be avoided. Unfortunately, existing legislation is unclear about how this conflict is to be resolved.

The tension between these rights exists both at the level of the EU and in the member states. The issue concerning EU institutions has arisen because neither the data protection regulation nor the data access regulation indicates clearly how the two regulations are to interrelate. As the European Data Supervisor has noted, "[i]t is not self-evident how the responsible Community authorities should act if the two

fundamental rights [to access data and protect data] apply at the same time …."[66] The issue concerning member states has arisen because the states must reconcile the data protection Directive with their own public access legislation. This section evaluates the relationship between data protection and data access in EU institutions, and it then turns to the same issue in member states.

___.31 EU Institutions

EU institutions have disagreed about the relationship between data protection and access regulations. In particular, the Ombudsman and the Supervisor have proposed different solutions concerning how the conflict between data access and protection should be reconciled.

___.311 The Data Access Exception

The data protection regulation 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* …."[67] EU institutions are therefore authorized to disclose personal data if such disclosure is required by the data access regulation. The data access regulation requires the disclosure of documents unless an exemption applies, and there is an exemption to protect personal privacy and integrity. That exception 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."[68]

There is a similar relationship between the Privacy Act and FOIA. The Privacy Act authorizes agencies to disclose personal information as required by the FOIA.[69] Exemption 6 of FOIA states that disclosure requirements do not apply to "matters that are… personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[70]

There is an important difference, however, between the US and the EU. Exemption 6 of FOIA tilts heavily in favor of disclosure. As indicated, FOIA requires disclosure of personal data unless it would "constitute a *clearly unwarranted* invasion of personal privacy." Understandably, the courts regard this language as favoring disclosure over the protection of privacy.[71] Thus, while the courts protect some private information, there

[66] European Data Protection Supervisor, Public Access to Documents and Data Protection 5 (July 2005), available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf.
[67] Commission Regulation 45/2001, art 5(a), 2000 O.J. (L8) 1, 5 (emphasis added)
[68] Commission Regulation 1049/2001, art. 4, 2001 O.J. (L. 145), 43, 45.
[69] 5 U.S.C. §552a(b)(2).
[70] 5 U.S.C. 552(6).
[71] *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 ….")

are also numerous examples of cases that refuse to block disclosure on privacy grounds.[72] By comparison, the privacy exception in the data access regulation does not contain the same tilt in favor of disclosure. If anything, it tilts the other way.

The exception for personal privacy in the data access regulation tilts in favor of protecting personal privacy for several reasons. 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."[73] Moreover, in contrast with other disclosure exceptions, the privacy exception is not subject to an overriding pubic interest in disclosure. 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*."[74] This language implies a balancing of the public interest against the protection of another interest that is not present in the privacy exception. 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.[75]

Finally, because the privacy exception to data access references the data protection regulation, it might be interpreted to forbid disclosure unless disclosure is permitted by the privacy regulation itself. According to the exception, an institution "shall refuse access to a document where disclosure would undermine the protection of … privacy and integrity of the individual, *in particular in according with the protection of personal data*."[76] Since under this interpretation the privacy regulation defines the scope of disclosure, personal data cannot be disclosed unless disclosure is permitted according to one of the exceptions found in the privacy regulation. If none of those exceptions apply, disclosure would be forbidden under the data access regulation as well as the privacy regulation.

Some decisions of the Commission appear to endorse this interpretation of the privacy exception. 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 the Data Protection Directive prevented it from disclosing the identities of the persons

---

[72] *See* LITIGATION UNDER THE FEDERAL OPEN GOVERNMENT LAWS 2004 (Harry A. Hammit, David L. Sobel, & Tiffany A. Steman, eds. 2004) at 161-170 (giving examples of records protected and not protected by Exemption 6).

[73] Commission Regulation 1049/2001, art. 4, 2001 O.J. (L. 145), 43, 45 (emphasis added).

[74] Commission Regulation 1049/2001, art. 4.1, 2001 O.J. (L. 145), 43, 45.

[75] *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.

[76] Commission Regulation 1049/2001, art. 4, 2001 O.J. (L. 145), 43, 45 (emphasis added).

concerned without their express permission.[77] As the reader may recall, the data protection regulation permits disclosure of personal data with the unambiguous consent of the data subject. 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.[78]

If, however, the privacy exception to the data access regulation is interpreted to permit disclosure only when it is permitted under the data protection regulation, the right to privacy becomes a substantial roadblock to transparency. Since such an approach gives little or no weight to the fundamental right of access to public documents, EU authorities have sought to interpret the privacy exception in a manner that avoids this restrictive result.

___.312 The Ombudsman

The Ombudsman has sought to reconcile the data access and data protection regulations by making a distinction between the protection of privacy interests relating to private and family life and relating to public activities. He interprets the privacy exception in the data access regulation to protect only data that relate to private and family concerns and not to information that relates to persons acting in a public capacity.

The Ombudsman's interest in this issue arose prior to the passage of the data protection regulation when he became involved in the matter described in the previous section involving Bavarian Lager, the German beer company. The company filed a complaint with the Ombudsman concerning the refusal of the Commission to disclose the names of the persons who attended the meeting organized by the Commission. In November, 2000, the Ombudsman ruled that the Commission should have released the information because it concerned a public activity.

The Ombudsman's decision drew on Article 7 of the Charter of Fundamental Rights of the European Union,[79] which he interpreted as limited to data concerning a person's private and home life. Article 7 reads: "Everyone has the right to respect for his or her private and family life, home, and communications."[80] The Ombudsman also justified his decision on the the right to public access:

---

[77] 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.

[78] 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.

[79] 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 ¶ ___, available at http://www.euro-ombudsman.eu.int/special/pdf/en/980713.pdf.

[80]

> Information supplied to an administrative authority by a person who participates in an administrative procedure does not seem to be "personal data" relating to that person merely by reason of the fact that he or she supplied it. The contrary view would imply that exists a fundamental right to supply information to an administrative authority in secret, which is not the case.[81]

Accordingly, the Ombudsman concluded "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 have been submitted to it concerning the exercise of its functions, nor the names of the persons who submitted the views or information."[82]

In November, 2001, the Ombudsman warned that "gains in openness achieved … in the public access regulation are under [a] threat … aris[ing] from the failure to understand the purpose and limits of data protection rules." The Ombudsman reiterated that to "interpret and apply data protection rules correctly, it is necessary to understand their legal basis and that they exist only to protect private and family life." He also warned that the "idea of striking a balance between" the right to access and the right to data protection "on a case-by-case basis whenever a name is mentioned misrepresents the nature both of dealing with openness in the public sector and the right to privacy." Finally, he indicated that his position did not mean that there may not be legal grounds to keep confidential data concerning an individual's public life, but that withholding the data had to be justified on the basis of one the exceptions to disclosure in the public access regulation other than the privacy exception. [83]

In December 2001, the European Parliament endorsed the Ombudsman's interpretation. The 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."[84]

__.312 Data Protection Supervisor

The Supervisor offers a different interpretation of the privacy exception in the data access regulation. This interpretation rejects the Ombudsman's categorical distinction between personal information relating to a person's privacy and family life and information relating to actions in a public capacity. Instead, the Data Supervisor proposes that public

---

[81] 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 ¶ 2.4, available at http://www.euro-ombudsman.eu.int/special/pdf/en/980713.pdf.
[82] *Id.* at ¶ 2.7.
[83] The European Ombudsman Letters and Notes: The Misuse of Data Protection Rules in the European Union (Sept. 9, 2002), available at http://www.euro-ombudsman.eu.int/letters/en/20020925-1.htm.
[84] 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=18020412875500000020200l-12-140i

officials have a right to privacy at governmental workplaces which may prevent the disclosure of some personal data in their employer's possession. At the same time, the Data Supervisor rejects the conclusion that the right to privacy always extends to people acting in a public capacity.[85]

Like the Ombudsman, the Data Supervisor starts with the language of the privacy exception, which requires institution to refuse "access to a document where disclosure would *undermine* the protection of … *privacy* and integrity of the individual …."[86] Although the exception is stated in absolute terms, the Supervisor notes that it only forbids disclosure if the "privacy" of the data subject is at stake and if public access to personal data would "undermine" that privacy right.[87] In order to determine when this occurs, the Data Supervisor looks to judicial interpretation Article 7 of the Charter of Fundamental Rights of the European Union. The heading of Article 7 reads "Respect for private and family life," and the text reads "Everyone has the right to respect for his or her private and family life, home and communications."[88]

According to the Supervisor, the courts, despite the previous language, have not interpreted Article 7 as only applying to privacy for private and family life.[89] The Supervisor cites the the *Niemietz*[90] and *Amann*[91] cases in the European Court of Human Rights as stating the notion of "private life" may cover a private business, public or any other environment. He argues this position was endorsed by the the European Court of Justice in the *Österreichischer Rundfunk and Others* case.[92] In *Amann*, the Court of Human Rights stated:

> The expression of 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 to be no reason in principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature.[93]

---

[85] European Data Protection Supervisor, Public Access to Documents and Data Protection §4.3.3 (July 2005), available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf.
[86] Commission Regulation 1049/2001, art. 4, 2001 O.J. (L. 145), 43, 45 (emphasis added).
[87] European Data Protection Supervisor, Public Access to Documents and Data Protection §2.4.4 (July 2005), available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf.
[88] Charter of Fundamental Rights of the European Union, art. 7, 2000/C 364/01, available at http://www.europarl.eu.int/charter/pdf/text_en.pdf.
[89] European Data Protection Supervisor, Public Access to Documents and Data Protection §3.2.2 (July 2005), available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf.
[90] Judgment of 16 December 1992, A-251.B, point 33.
[91] Judgment of 16 February 2000, Reports 2000-H.
[92] Judgment of the Court of 20 May 2003, Joined cases C-465/00, C-138/01 and C-139/01. ECR 2003, Page I-4989, Paragraph __.
[93] Judgment of 16 February 2000, Reports 2000-H.

While the Supervisor seeks to give a broad interpretation to the right to privacy, he is unwilling to endorse absolute protections for privacy rights in the context of data access. He argues that European case law and the principle of proportionality both require that consideration be given to the interest in transparency when the exception is interpreted. Cases such as *Council v. Hautala*,[94] for example, require that exceptions to a fundamental right should be strictly construed and applied so as not to defeat the application of the fundamental right.[95] The principle of proportionality further requires "that derogations remain with the limits of what is appropriate and necessary for achieving the aim in view."[96]

In light of the importance of honoring the right to data access, the Supervisor offers a narrowing interpretation of the privacy exception in the data access regulation. The "mere fact that a document contains personal data," he contends, "does not mean that a person's privacy is involved."[97] Disclosure may not undermine a person's privacy interests because there is no legitimate expectation of privacy in some contexts of public life. Public officials and employees cannot have a legitimate expectation of *complete* privacy because they are in a different position than persons working for private concerns. They are in a different position because

> [e]mployees in public administration must be aware for several reasons, their personal data may be of public interest to a degree different from the situation where he or she would be working in the public sector. Two such interests are accountability and transparency. For these reasons, certain personal data (such as the name and function of an official) can, in general, be disclosed without consent, provided that it is appropriate and motivated by the activities of the institution.[98]

Nevertheless, there is also a legitimate expectation of privacy in some aspects of public life because of the nature of the information involved. For example, the Supervisor recommends that data would normally fall with the scope of the privacy exception of the public access regulation if:

- sensitive data as mentioned in Article 10 of Regulation 45/2001 are involved, such as for instance data concerning health;
- the honour and reputation of a person is involved;

[94] Judgment of the Court, Council of the European Union v. Heidi Hautala, C-353/99 P, ECR [2001], p. I-9565.
[95] European Data Protection Supervisor, Public Access to Documents and Data Protection §2.4.4 (July 2005), available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf.
[96] *Id.*
[97] European Data Protection Supervisor, Public Access to Documents and Data Protection §4.3.1 (July 2005), available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf
[98] European Data Protection Supervisor, Public Access to Documents and Data Protection §4.3.3 (July 2005), available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf.

- a person could be placed in a false light;
- embarrassing facts would be disclosed
- information given or received by the individual confidentially would be disclosed.

When information is protected from disclosure by the privacy exception of the data access regulation, the Supervisor argues that an institution can only withhold those portions of the document that undermine the privacy interest. This conclusion is based on the proportionality principle because it requires that derogations of a fundamental right are not permitted if the government's objectives can be achieved by other less restrictive measures. Thus, EU institutions should comply with the privacy exception to the public access regulation by redacting only those portions of a document that would undermine a person's privacy rights.[99] The Supervisor acknowledges that the courts have ruled that redaction is not necessary when it results in an unreasonable amount of work, but that he contends this qualification is limited to "exceptional circumstances."[100]

Finally, the Supervisor points out the data privacy regulation permits the disclosure of non-sensitive information covered by the regulation if there is express consent by the data subject.[101] He recommends that EU institutions seek such permission any time that they acquire personal data that is likely to be of interest to the public.[102]

__.32 Member States

The tension between data protection and data access is also present in the member states. How the member states resolve this tension is impacted by Directive 95/96. According to the Data Protection Working Group, Directive 95/96 both authorizes the disclosure of personal data as required by a member state's data access legislation and limits the limits the extent to which a member can authorize the disclosure of personal data in such legislation.

Article 7(c) of the Directive authorizes a controller to process personal data as "necessary for compliance with a legal obligation to which the controller is subject."[103] While this provision appears to authorize the disclosure of personal data whenever another law requires it, the Working Group contends Directive 95/96 does not permit the exception to swallow the rule. The Working Group interprets Article 7(c) of the Directive as also

[99] European Data Protection Supervisor, Public Access to Documents and Data Protection §4.3.5 (July 2005), available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf.
[100] European Data Protection Supervisor, Public Access to Documents and Data Protection §4.2.3 (July 2005), available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf.
[101] *See* note __ & accompanying text.
[102] European Data Protection Supervisor, Public Access to Documents and Data Protection §5.2 (July 2005), available at http://www.edps.eu.int/publications/policy_papers/Public_access_data_protection_EN.pdf.
[103] Council Directive 95/46, Art. 7(c), 1995 O.J. (L 281) 31, 40.

limiting the authority of member state to authorize disclosure of personal data in domestic legislation.[104]

Article 7(c) has this effect because, while it authorizes disclosure of information according to a member state's laws, it also requires a member state to comply with Directive 95/96. Thus, if 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 95/96 since it would in the position of permitting the disclosure of personal data without regard to the protections required by Directive 95/96. As the Working Party explains,

> Given the obligation of administrations to grant public access to documents is limited by their obligation to protect personal data, an unrestricted, automatic, unfettered public disclosure of personal data held by an administration … would not be compliant with a legal obligation to which the administration would be subject…. In other words, the compliance with a legal obligation cannot be used as a proper ground to make automatic, unrestricted public disclosure of personal data according to the Directive.[105]

According to the Working Party, Article 7(f) confirms the previous interpretation.[106] 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)."[107] 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."[108]

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

---

[104] 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.

[105] 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.

[106] 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.

[107] Council Directive 95/46, Art. 7(f), 1995 O.J. (L 281) 31, 40.

[108] Council Directive 95/46, Art. 1(1), 1995 O.J. (L 281) 31, 38.

satisfied or rejected."[109] 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.[110]

[109] 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.

[110] *Id.*