A Primer for Data-Protection Principles in the European Union

Harvey L. Kaplan

Mark W. Cowing

Gabriel P. Egli

Shook, Hardy & Bacon L.L.P.

2555 Grand Boulevard
Kansas City, Missouri, USA 64108-2613
(816) 474-6550
hkaplan@shb.com

Return to course materials table of contents

Harvey L. Kaplan is a partner in the Kansas City, Missouri office of Shook, Hardy & Bacon LLP. He chairs the firm's Pharmaceutical and Medical Device Litigation Division and has served as a member of its Executive Committee. He has tried high profile cases in many jurisdictions, and has defended pharmaceutical and medical device companies in numerous national products liability litigations. Mr. Kaplan is a member of many professional organizations, and has served on the Boards of Directors of DRI and IADC. He is a Fellow of the International Academy of Trial Lawyers and of the International Society of Barristers. Mr. Kaplan has been at the forefront of launching DRI Europe. He frequently speaks and writes on products liability topics. He is a former Chair of the DRI Drug and Medical Device Committee.

Mark W. Cowing is Of Counsel and Gabriel Egli is an associate in the Kansas City office of Shook, Hardy & Bacon, LLP. Mr. Cowing is a member of the firm's eDiscovery, Data and Document Management Practice, and is a frequent speaker on technology matters. Mr. Egli's practice areas include pharmaceutical and medical device defense.

A Primer for Data-Protection Principles in the European Union

Table of Contents

A Primer for Data-Protection Principles in the European Union

I. European Perspective Regarding Protection of Personal Data

Throughout Europe, the privacy of personal information and data is considered a fundamental human right. As such, it is the subject of a complex and comprehensive network of legislation, which, not surprisingly, significantly impacts both business practices and litigation. A basic understanding of data protection law is, therefore, essential for any legal practice that operates in Europe or represents business clients there. A review of the Data Protection Directive implemented in the European Union ("EU") provides a useful guide to the types of principles that govern data protection in Europe.

II. Historical Origins of European Protection of Personal Data

Over the course of the Twentieth Century, Europeans became acutely familiar with the dangers posed by unrestricted access to personal information. Authoritarian regimes across the continent often collected and used personal information to devastating effect. These experiences animated efforts to prevent the unchecked use of personal data.[1]

The European Convention of Human Rights of 1950 ("ECHR") represented one of the first efforts to extend protection to personal data.[2] Article 8 of the ECHR provides that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[3] It further provides that interference with the right by governments is prohibited except where necessary for the proper function of a democratic society.[4]

The right and concept of privacy was further outlined in the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("Guidelines") that were issued by the Organization for Economic Cooperation and Development ("OECD") in 1980.[5] The Guidelines, which represented an effort to reduce barriers to the free flow of information that arose from divergent national laws, defined "personal data" as "any information relating to an identified or identifiable individual."[6] In addition, the Guidelines outlined several basic principles for the protection of personal data as well as for the free flow of information among member states. The lack of any binding force behind the Guidelines, however, meant that they had little effect in unifying inconsistent data protection laws.

III. The Current Approach to Protecting Personal Data—Directive 95/46/EC

The European Union's current data protection regime is built upon Directive 95/46/EC (the "Directive"). The Directive took effect on October 25, 1998—three years after it was formally approved.[7] Its purpose is twofold.[8] First, the Directive seeks to guarantee adequate protection of a fundamental right by establishing minimum standards for the use of personal data. Second, the Directive seeks to harmonize the data protection laws of member states—a move intended to remedy the persistence of divergent data protection regimes that hindered the realization of the common market contemplated by the Treaty of Rome.

A. Scope of Directive 95/46/EC

Although the Directive represents a comprehensive approach to governing the use of personal data, it does not apply in two relatively narrow contexts.[9] First, the Directive does not apply to activities that are outside the scope of Community law. These activities include "processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State

security matters) and the activities of the State in areas of criminal law."[10] Second, the Directive does not apply to processing by an individual engaged in "purely personal or household activity."[11] Such activities include, for example, the use of a computerized spreadsheet to create a mailing list for birthday-party invitations or graduation announcements. The existence of only two exceptions demonstrates the Directive's remarkable scope.

B. Implementation of Directive 95/46/EC

The Directive itself does not impose obligations directly on people or businesses. Instead, it requires that each EU member state[12] enact laws that govern the processing of personal data, and that satisfy certain minimum standards.[13] These minimum standards are outlined in the sections that follow. To date, all member states have enacted laws in accordance with the Directive.[14] To monitor and enforce these laws, each EU member state must create a data protection authority.[15]

C. Penalties for Violating Directive 95/46/EC

Violations of the Directive may implicate two levels of liability. First, they may result in sanctions from a data protection authority or from a judicial authority. The Directive requires that each member state establish sanctions for the infringement of its provisions.[16] These sanctions may take the form of fines and/or imprisonment.[17] Second, they may result in civil liability to a data subject. The Directive's provisions are backed by a requirement that member states "provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered."[18]

IV. Personal Data—Directive 95/46/EC

The range of data to which the Directive applies is, by definition and design, remarkably broad. The Directive defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject')."[19] This definition is not limited to electronic forms of data. Instead, it reaches written information, photographs, and even sound recordings of identified or identifiable people.

The Directive further defines an "identifiable person" as "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[20] As a result, the Directive may even encompass such things as Internet protocol ("IP") addresses. Although IP addresses—which consist of a series of numbers—may not directly identify the user, they may provide sufficient information to indirectly determine the user's identity.

V. Processing—Directive 95/46/EC

The range of activities to which the Directive applies is also remarkably broad. The Directive defines "processing" as "any operation or set of operations that 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."[21] This definition reaches essentially every task a party or its counsel undertakes to process data in the course of litigation. In fact, as noted, the mere act of storing personal data implicates the requirements of the Directive.

For the purposes of the Directive, 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"

is considered a "controller."[22] This definition may reach people performing such seemingly innocuous activities as recording the names and addresses of business contacts in a data organizer.[23] Such controllers are subject to specific obligations, which are addressed in greater detail below. In light of the expansive definitions of "processing" and "controller," it is essential to understand how and when processing is permitted.

A. Principles Relating to Data Quality (How to Process Personal Data)

The Directive provides several data quality principles that outline how personal data must be handled:

1) *Fair and Legal*—Personal data must be "processed fairly and lawfully."[24] Although the lawfulness requirement is straightforward, the fairness requirement is not. In effect, the requirement that data processing be fair acts as a sort of legal catchall. While some countries have taken steps to define the fairness requirement, others leave it to the discretion of the data protection authorities.[25]
2) *Purpose-Limited*—Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[26]
3) *Relevant*—Personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[27]
4) *Accurate*—Personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data that are inaccurate or incomplete, having regard for the purposes for which they were collected or for which they are further processed, are erased or rectified."[28]
5) *Time-Limited*—Personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."[29]

B. Criteria for Legitimate Data Processing (When Processing Is Permitted)

Although the Directive generally prohibits the processing of personal data, it outlines several conditions under which such processing is permitted:

1) *Consent*—Personal data may be processed when "the data subject has unambiguously given his consent."[30] The Directive further specifies that consent must be both informed and voluntary.[31] Although this condition appears straightforward, it may prove problematic in practice. To begin, certain types of personal data may require the consent of multiple people. Electronic mail ("e-mail"), for example, involves the identity of at least two people, the sender and recipient. Moreover, certain member states may have different standards for what constitutes "unambiguous" consent. German authorities, for example, have suggested that "[i]t is doubtful as to whether consent can be granted voluntarily in an employment relationship."[32]
2) *Contract*—Personal data may be processed when "necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."[33] This provision clearly applies to processing that is strictly necessary to achieve the specific purpose of the contract. What is less clear is whether it applies to requests for processing that are incorporated into non-negotiable contacts, but are not essential to performance of the contract.[34] Whether such contractual provisions are enforced may depend on specific circumstances and specific data protection law.
3) *Legal Obligations*—Personal data may be processed when "necessary for compliance with a legal obligation to which the controller is subject."[35] Despite the plain wording of this provision, it is

possible that some legal obligations may not justify processing of personal data. Although the provision certainly applies to legal obligations arising within the EU, it is not entirely clear that it applies to legal obligations arising elsewhere.[36]

4) *Vital Interests*—Personal data may be processed when "necessary in order to protect the vital interests of the data subject."[37]

5) *Public Interest*—Personal data may be processed when "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed."[38]

6) *Legitimate Interests*—Personal data may be processed when "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)."[39] The type of balancing of interests provided in this provision grants member states significant flexibility in determining when processing is permitted. As such, individual data protection laws outline the precise scope of when such processing is "necessary."

VI. Processing Sensitive Data—Directive 95/46/EC

The Directive adds an additional layer of protection to personal data considered uniquely sensitive. This type of personal data includes "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[40] Processing of such data is prohibited except in a limited set of circumstances. Those circumstances exist where:

1) a data subject has given explicit consent,[41]

2) necessary for controller to meet legal obligations with respect to employment law,[42]

3) necessary to protect the vital interests of a data subject (or another person), and the data subject is physically or legally incapable of giving consent,[43]

4) carried out by a non-profit organization whose aim is to advance an agenda related to one of the categories of sensitive data,[44]

5) the data are manifestly made public by the data subject,[45]

6) necessary to establish or defend legal claims,[46] and

7) required by a health professional in the course of providing treatment or managing health-care services.[47]

VII. Rights of Data Subjects—Directive 95/46/EC

In addition to outlining how and when personal data may be legally processed, the Directive also establishes that data subjects are to enjoy certain rights.

1) Right of Access—Data subjects have the right to obtain information regarding:
   a) whether their personal data is being processed,
   b) the content and source of any personal data undergoing processing, and
   c) the purpose of any such processing.[48]

2) Right to Correct—Data subjects have the right to correct, erase, or block the transfer of inaccurate or incomplete data.[49]

3) Right to Object—Data subjects have the right to "object at any time on compelling legitimate grounds relating to [their] particular situation to the processing of data relating to [them], save where otherwise provided by national legislation."[50] Data subjects also have the right to object "to the processing of personal data relating to [them] which the controller anticipates being processed for the purposes of direct marketing."[51]

VIII. Obligations of Controllers—Directive 95/46/EC

In addition to specifying how and when personal data may be processed, the Directive also imposes other obligations on controllers. These additional obligations relate to notice—to data subjects, and to data protection authorities.

A. Notice to Data Subjects

Except where a data subject already has such information, controllers must provide the data subject with the following information: 1) the identity of the controller; 2) the purpose of the processing; 3) the recipients or "categories of recipients" of the data; 4) whether providing information is obligatory or voluntary (including an explanation of the consequences of failure to provide the information); and 5) the existence of the right to access and correct personal data.[52]

B. Notice to Data Protection Authorities

Except where national law provides an exemption, controllers must provide the relevant data protection authorities with the following information prior to performing any automatic processing operation:

1) the name and address of the controller and any relevant representative;
2) the purpose(s) of the processing;
3) a description of the category or categories of persons affected, and of the data relating to them;
4) the recipients or "categories of recipients" to whom the data may be disclosed;
5) any proposed transfers to third countries; and
6) a general description of measures taken to ensure the security of processing.[53]

IX. Transfers of Personal Data to Third Countries

To ensure that controllers could not circumvent the Directive merely by transferring data outside of the EU for processing, the Directive expressly prohibits the transfer of personal data to third (non-EU) countries except under limited circumstances. This restriction gives the Directive *de facto* extraterritorial effect. For example, many multinational businesses are forced to ensure that all of their data processing activities are performed in accordance with the terms of the Directive because of the difficulty or impossibility of separating personal data collected within the EU from personal data collected elsewhere.[54]

The exceptions to the general prohibition against transferring personal data outside of the EU fall into the following categories: country-specific, business-specific, and circumstance-specific.

A. Country-Specific Exceptions

The Directive itself provides only one country-specific exception. This exception, however, does not currently permit transfers of personal data to the United States. To address the potentially crippling effect this prohibition would have on international business transactions, a second exception was created.

1. Adequate Level of Protection

Article 25 of the Directive provides that the transfer of personal data may take place where "the third country in question ensures an adequate level of protection." Determinations regarding which countries provide the requisite level of protection are made by the EU Commission with recommendations from a Working Party established pursuant to Article 29 of the Directive.[55] In practice, few countries provide the requisite level of protection. Among the countries that do are the three non-EU members of the European Economic Area ("EEA"): Norway, Liechtenstein, and Iceland. The only additional countries that the Commission has determined provide an adequate level of protection are Switzerland, Canada, Argentina, Guernsey, and the Isle of Man. Not surprisingly, the United States is absent from this list.

2. Safe Harbor (Exclusive to the United States)

The EU and the United States Department of Commerce reached an agreement in 2000 that permits the transfer of personal data from the EU to organizations in the U.S. that publicly certify themselves to be a Safe Harbor.[56] The Safe Harbor process permits a U.S. company or affiliate to receive personal data from the EU if it agrees to treat the data as if the Directive applied. Personal data transferred to a Safe Harbor organization may, for example, include payroll data, employee evaluations, customer lists, billing information, and documents collected for production in litigation within the U.S.

As part of the Safe Harbor process, an organization must comply with the following seven principles that mirror principles outlined in the Directive:

1) Notice;
2) Choice;
3) Onward Transfer;
4) Security;
5) Data Integrity;
6) Access; and
7) Enforcement.[57]

In addition, to become certified for Safe Harbor status, an organization must complete and submit to the Department of Commerce a form that provides contact information, a description of how the organization will process personal data received from the EU, and a summary of data-handling policy. An organization must resubmit and update this information annually to remain certified.[58]

B. Business-Specific Exceptions

There are currently two methods that businesses (regardless of where they are based) can employ to avoid the prohibition against transferring personal data outside of the EU. These methods—standard contractual clauses and binding corporate rules—are likely to become increasingly important as data protection authorities institute stricter enforcement regimes for cross-border transfers of personal data.

1. Standard Contractual Clauses

Pursuant to Article 26(2) of the Directive, the EU Commission has established three sets of pre-approved contractual clauses that, when executed by a data exporter and a data importer, permit transfer of specific personal data outside the EU.[59] Despite pre-approval from the Commission, as a practical matter, some data protection authorities still require approval of the contractual clauses before transfer is permitted. The use

of such standard clauses contractually binds the party importing personal data to a set of rules that are similar to the principles that apply to the Safe Harbor process. In addition, the standard clauses specifically provide that a contracting party is liable for any damage suffered by the data subject (who is considered a third-party beneficiary) as a result of that party's breach.

2. Binding Corporate Rules

The second business-specific exception relies on so-called Binding Corporate Rules ("BCRs"). This exception is available to multinational corporations that enact codes of conduct that comply with the Directive, and that apply company-wide. Once the BCRs are approved, they allow a corporation to freely transfer personal data throughout its organization.

The approval process for BCRs begins with an application to the most appropriate data protection authority. The application must detail the applicant's efforts to protect and process personal data worldwide. In addition, the application must demonstrate that the systems necessary to protect and process the data are already functional and effective. After the first data protection authority provisionally approves the application, the application is sent to every other relevant data protection authority for approval.

C. Circumstance-Specific Exceptions

The circumstance-specific exceptions to the general prohibition against transferring personal data outside of the EU are similar to the circumstances that determine when such personal data may be processed.

1) *Consent*—Transfer of personal data may occur where the data subject has given unambiguous consent.[60]
2) *Contract*—Transfer of personal data may occur where "necessary for the performance of a contract between the data subject and controller,"[61] or where "necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party."[62]
3) *Public Interest*—Transfer of personal data may occur where "necessary or legally required on important public interest grounds."[63]
4) *Legal Claims*—Transfer of personal data may occur where necessary to establish or defend legal claims.[64]
5) *Vital Interests*—Transfer of personal data may occur where "necessary in order to protect the vital interests of the data subject."[65]
6) *Transfer from Register*—Transfer of personal data my occur where it is made from a "register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest."[66]

X. Conclusion

Personal data is the subject of extensive legislation in the EU. Although the details of national laws regarding data protection vary, Directive 95/46/EC outlines the basic parameters within which these laws operate. Because business and litigation necessarily involve the use of such personal data, a basic understanding of personal data protection is essential in representing clients who may be affected.

Endnotes

[1] *See* Ryan Moshell, *. . . And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 Tex. Tech. L. Rev. 357, 358 (2005); Marsha Cope Huie et al., *The Right to Privacy in Persona Data: The EU Prods the U.S. and Controversy Continues*, 9 Tulsa J. Comp. & Int'l L. 391, 441-42 (2002).

[2] *See* The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and E-Discovery 10-11 (Public Comment Version, August 2008).

[3] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms as Amended by Protocol No. 11, art. 8 (Sept. 2003), available at http://www.echr.coe.int/ECHR.

[4] Article 8 permits interference where necessary in the interests of "national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." *See id.*

[5] Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 Ind. L. Rev. 173,180 (1999).

[6] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1(b) (Sept. 23, 1980), available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[7] Directive 95/46/EC, art. 32, 1995 O.J. (L 281) 31, 50 (EC), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML; Cate, *supra* note 5, at 182.

[8] Directive 95/46/EC, *supra* note 7, at art. 1.

[9] *Id*. at art. 3.

[10] *Id*.

[11] *Id*.

[12] The European Union consists of the following twenty-seven nations: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

[13] Directive 95/46/EC, *supra* note 7, at recital 69, art. 5.

[14] For a list of the specific laws in effect for each member state, see European Commission: Justice and Home Affairs: Data Protection: Status of Implementation, http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm.

[15] Directive 95/46/EC, *supra* note 7, at art. 28.

[16] *Id*. at art. 24.

[17] For example, Germany has provided for administrative fines of up to €250,000 per violation—the highest administrative fine in the EU. *See* Breon S. Peace & Jennifer A. Kennedy, *The Impact of EU Data Protection Laws on U.S. Government Enforcement Investigations*, 18 Int'l HR J. 2 (Winter 2009). In addition to providing for fines, French law permits imprisonment for up to five years. *See* CNIL—*Data Protection Act: The Principles*, http://www.cnil.fr/index.php?id=41 (last visited Feb. 28, 2009). For a description of sanctions in force in the various EU member states, see Data Protected. Linklaters, https://clientsites.linklaters.com/Clients/dataprotected/Pages/index.aspx (last visited Feb. 28, 2009).

[18] *Id*. at art. 23(1).

[19] *Id*. at art. 2(a).

[20] *Id*.

[21] *Id*. at art. 2(b).

[22] *Id*. at art. 2(d).

[23] *See* Cate, *supra* note 5, at 183.

[24] *Id*. at art. 6(1)(a).

[25] Douwe Korff, *Data Protection Laws in the European Union* 37-38 (Richard Hagle ed., Federation of European Direct and Interactive Marketing and The Direct Marketing Association 2005).

[26] Directive 95/46/EC, *supra* note 7, at art. 6(1)(b).

[27] *Id*. at art. 6(1)(c).

[28] *Id*. at art. 6(1)(d).

[29] *Id*. at art. 6(1)(e).

[30] *Id*. at art. 7(a).

[31] *Id*. at art. 2(h).

[32] Düsseldorfer Kreis Ad-Hoc Working Group on Employee Data Protection, Whistleblowing—hotlines: *Internal Warning Systems and Employee Data Protection* 4 (April 19-20, 2007), available at http://www.globalcompliance.com/pdf/german-guidelines-english-translation.pdf.

[33] Directive 95/46/EC, *supra* note 7, at art. 7(b).

[34] *See* Korff, *supra* note 25, at 42. Such contractual provisions may include authorizations to allow third parties to access personal information for marketing purposes.

[35] Directive 95/46/EC, *supra* note 7, at art. 7(c).

[36] *See* John D. Kinton, *Managing the EU-US Discovery Conflict*, Law 360, Oct. 16, 2008, http://health.law360.com/print_article/72082.

[37] Directive 95/46EC, *supra* note 7, at art. 7(d).

[38] *Id*. at art. 7(e).

[39] *Id*. at art. 7(f).

[40] *Id*. at art. 8(1).

[41] *Id*. at art. 8(2)(a).

[42] *Id*. at art. 8(2)(b).

[43] *Id*. at art. 8(2)(c).

[44] *Id*. at art. 8(2)(d).

[45] *Id*. at art. 8(2)(e).

[46] *Id*.

[47] *Id*. at art. 8(3).

[48] *Id*. at art. 12(a).

[49] *Id*. at art. 12(b).

[50] *Id*. at 14(a).

[51] *Id*. at art. 14(b).

[52] *Id*. at arts. 10, 11.

[53] *Id*. at arts. 18, 19.

[54] Cate, *supra* note 5, at 184.

[55] S*ee* Directive 95/46/EC, *supra* note 7, at arts. 25(b), 29-30.

[56] Export.gov, Safe Harbor Overview, http://www.export.gov/safeharbor/SH_Overview.asp (last visited Feb. 9, 2009).

[57] *See id*.; Export.gov, Safe Harbor Privacy Principles, http:www.export.gov/safeharbor/eu/sh_en_privacy1.asp (last visited Feb. 20, 2009).

[58] Export.gov, Safe Harbor Overview, *supra* note 56.

[59] Directive 95/46/EC, *supra* note 7, at art. 26(2). The three sets of standard contractual clauses are presented as annexes to the following Commission Decisions:

1. Decision 2004/915/EC, 2004 O.J. (L 385) 74-84 (EC), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF;

2. Decision 2002/16/EC, 2002 O.J. (L 6) 52-62 (EC), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF; and

3. Decision 2001/497/EC, 2001 O.J. (L 181) 19-31 (EC), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:EN:PDF.

[60] Directive 95/46/EC, *supra* note 7, at art. 26(a).

[61] *Id*. at art. 26(b).

[62] *Id*. at art. 26(c).

[63] *Id*. at art. 26(d).

[64] *Id*.

[65] *Id*. at art. 26(e).

[66] *Id*. at art. 26(f).

Return to course materials table of contents