Volume 41 | Issue 1 Article 7

1996

European Union Directive on Personal Privacy Rights and Computerized Information

Rosario Imperiali d'Afflitto

EUROPEAN UNION DIRECTIVE ON PERSONAL PRIVACY RIGHTS AND COMPUTERIZED INFORMATION*

ROSARIO IMPERIALI D'AFFLITTO**

I. INTRODUCTION

IN the last fifteen years, domestic and international European lawmakers have attempted to address the protection of individuals ("data subjects") with regard to automatic processing of personal data. Opened for signature on January 28, 1981, the European Convention for the Protection of Individuals With Regard to the Automatic Processing of Personal Data ("Convention") spurred many European nations to take legislative action within their borders on this subject.[1] Contingent upon a particular state's proper ratification of and adherence to the Convention, these new laws opened the door for local implementation of the Convention's principles.[2] Today, despite the lack of any real supranational legal coordination, European national laws on data privacy are essentially the same, as they are based upon the Convention's principles.

Because most European states' data privacy laws arise from a

* This Recent Development is available at the *Villanova Law Review* home page at http://vls.law.vill.edu/academic/jd/journals/law-review/Volume_41/.

** Rosario Imperiali d'Afflitto currently practices as an attorney-at-law, specializing in business, copyright, computer and European antitrust law. He received his Law Degree from the University of Naples (*summa cum laude*) and formerly served as Senior Counsel for IBM and ISSC Italia, a wholly owned IBM subsidiary.

1. European Convention for the Protection of Individuals With Regard to the Automatic Processing of Personal Data, *signed on* Jan. 28, 1981, Europ. T.S. 108, 20 I.L.M. 317 [hereinafter Convention] (entered into force Oct. 1, 1985).

2. Of the European Union member states, only Greece and Italy have not yet ratified the Convention. The Italian Parliament, with law n.98 of February 21, 1989, authorized the ratification of the Convention; entry into force, however, will be subject to adoption by the Parliament of "the necessary measures in its domestic law to give effect to the basic principles for data protection set out" in the Convention (Article 4(1)). Convention, *supra* note 1, art. 4(1). Thus, a data privacy law is still to be enacted in Italy. For the same reason, Italy has not been able to implement the Schengen Agreement on the Gradual Abolition of Checks at Their Common Borders among the signatory states, despite the fact that this treaty has been ratified by law 388 of September 30, 1993. *See* Schengen Agreement on the Gradual Abolition of Checks at Their Common Borders, June 14, 1985, 30 I.L.M. 68 [hereinafter Schengen Agreement]. A condition precedent to the Schengen Agreement is, in fact, adoption of a national law implementing the Convention. *See* Convention Applying the Schengen Agreement of June 14, 1985 on the Gradual Abolition of Checks at Their Common Borders, June 19, 1990, 30 I.L.M. 84 [hereinafter Schengen Convention].

common source,[3] the need for a European Directive on this subject may not have been self-evident. Three continuing problems, however, showed the underlying need for a Directive in this field. Specifically, a Directive was needed to address: (1) the divergences still present in the national laws of the European Union (E.U.) member states; (2) the absence of specific legislation on this matter with regard to at least two member states, Greece and Italy; and (3) the absence of a supranational supervisory body.

In recognition of this need, on July 24, 1995, the E.U. Council approved the Directive. On October 24, following the co-decision procedure, the Directive was signed by the Presidents of both the E.U. Council and Parliament. Member states now have until October 23, 1998 to adopt the Directive into their national legal systems.

This Recent Development discusses Directive No. 95/46/EC of the E.U. "on the protection of individuals with regard to the processing of personal data and on the free movement of such data," adopted by the E.U. Parliament and Council of Ministers on October 24, 1995 ("Directive").[4] After explaining the need for the Directive, this article analyzes the Directive's general principles and scope. This article also details the Convention principles that member states must adopt domestically without modifications, as well as those principles member states may exercise discretion in adopting.

3. The following table summarizes the data privacy laws of E.U. member states.

E.U. Member State	Date enacted	Date in force	Convention ratified	Registration Notification	Manual Records	Legal Persons
Austria	10/18/78	01/01/80	Yes	All data	Yes	Yes
Belgium	12/08/92	04/01/93	No	Some data	Yes	No
Denmark	06/08/78	01/01/79	Yes	Some data	Yes	Yes
Finland	02/04/87	01/01/88	Yes	Some data	Yes	No
France	01/06/78	01/01/80	Yes	All data	Yes	Yes
Germany	01/27/77	01/01/79	Yes	Some data	Yes	No
Ireland	07/13/88	04/19/89	Yes	Some data	No	No
Luxembourg	03/31/79	10/01/79	Yes	All data	No	Yes
Netherlands	12/28/88	07/01/90	Yes	Some data	Yes	No
Norway	06/09/78	01/01/80	Yes	Some data	Yes	Yes
Spain	10/29/92	02/01/93	Yes	All data	No	No
Sweden	05/13/73	07/01/74	Yes	All data	No	No
U.K.	07/12/84	11/11/87	Yes	All data	No	No

STEWART DRESNER, PRIVACY LAWS & BUSINESS (1994). For a discussion of the situation in Italy and Greece, see *supra* note 2.

4. Council Directive No. 95/46/EC 1995 O.J. (L 281) (Nov. 23, 1995) [hereinafter Directive]. The first proposal of the E.U. Commission on this subject dates back to the year 1990. *See* Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data COM/90/314, 1990 O.J. (C 277) (Nov. 5, 1990) [hereinafter Proposal].

II. THE NEED FOR A EUROPEAN UNION DIRECTIVE ON DATA PRIVACY

A. *Divergences Still Existing Among European National Laws on Data Privacy*

In addition to jeopardizing the harmonization of member states' legislation on important matters according to the Treaty of Rome,[5] divergences still existing among the various national laws[6] may also prevent transborder data flow, thus creating a barrier to the four basic freedoms of movement set forth in the Treaty.[7] As a result, these divergences also impinge upon the Directive. The third "Whereas" to the Directive asserts that "the establishment and functioning of an internal market in which, in accordance with Article 7A of the Treaty of Rome, the free movement of goods, persons, services and capital is ensured require . . . that personal data should be able to flow freely from one Member State to another."[8] Because of the reciprocity principle present in almost all E.U. member states' data privacy laws, the differing national systems of protection may prevent this free flow of personal data.[9] According to the reciprocity principle, the state from which data will be transmitted can prohibit the flow if the receiving state does not guarantee adequate protection.[10]

---

5. Treaty Establishing the European Community, Mar. 25, 1957, 298 U.N.T.S. 11 [hereinafter Treaty of Rome].

6. For example, while United Kingdom law on data privacy refers only to automated personal data, corresponding Belgian, French, German and Spanish laws also include manually recorded personal data structured according to specific criteria. At the same time, German law does not discriminate between personal data in general and "sensitive" data (i.e., those "personal 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"). France, the United Kingdom, Spain and other E.U. member states, however, do regulate "sensitive" data more restrictively. Finally, Austrian, Luxembourg, French, Danish and Norwegian laws also protect legal entities' right to privacy, thus including in the definition of data any information relating to an identified legal person. The vast majority of the remaining E.U. member states regulate only data related to natural persons.

7. The Treaty of Rome states that "[t]he internal market shall comprise of an area without internal frontiers in which the free movements of goods, persons, services and capitals is ensured in accordance with the provisions of this Treaty." Treaty of Rome, *supra* note 5, art. 7a.

8. Directive, *supra* note 4, at 3d "Whereas."

9. *Id.* at 7th & 8th "Whereas."

10. *See id.* at 57th "Whereas." The Directive further states that "in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States." *Id.* at 8th "Whereas."

B. *Absence of Specific Legislation on Data Privacy in Greece and Italy*

The absence of specific legislation on data privacy in Greece and Italy prevents standard implementation of the Convention among all E.U. member states. In addition, it impedes harmonization of member states' legislation and hinders the free flow of data over borders.[11] Accordingly, the need to have all member states implement domestically common rulings on data privacy also justified the adoption of an E.U. Directive.

C. *Creation of a Supranational Supervisory Body*

The creation of a supervisory body at a supranational level would contribute to the harmonization, consulting and sharing of experiences among the National Supervisory Authorities on Data Privacy. This would further harmonization at an administrative level, parallel to that sought by the European Council on a legislative level through the Directive.[12]

III. PRINCIPLES AND SCOPE OF THE DIRECTIVE

On July 24, 1995, the E.U. Council contradicted experts' timing forecasts and adopted Directive No. 95/46/EC. Most commentators predicted, however, that it would then stall between the Parliament and the Council.[13] It did not, however, and on October

11. The Italian Parliament's authorization (per law n.388 of September 30, 1993) of the ratification of the Schengen Agreement, of June 14, 1985, further stresses the urgency of enacting a data privacy law in Italy. The presence of a national law on data privacy protection is, in fact, a prerequisite for the above ratification. For a further discussion of the situation in Italy, see *supra* note 2.

12. The Directive states that "at a Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; . . . having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive." Directive, *supra* note 4, at 65th "Whereas." It further states that the Working Party "shall be composed of a representative of the supervisory authority . . . designated by each Member State and of a representative of the authority established . . . for the Community institutions and bodies, and of a representative of the [E.U.] Commission." *Id.* art. 29.

13. The Directive, in its final version, is the result of a second proposal from the E.U. Commission, presented on October 16, 1992. *See* 1992 O.J. (C 311) (Nov. 27, 1992). The first proposal is dated July 27, 1990. *See* Proposal COM/90/314, 1990 O.J. (C 277) (Nov. 5, 1990). The Parliament's first reading took place in the Spring of 1992. On February 20, 1995, the parties reached a common position. In June, at a second reading, the Parliament presented six amendments to the common position, which were subsequently accepted by the Commission. Seeking to avoid the lengthy procedure prescribed by Article 189B of the Treaty, which would apply if there were disagreement, and relying upon the amendments' non-funda-

24, Parliament adopted the Directive. The details of the Directive are discussed below.

A. *Freedom of Information and Protection of Privacy*

Through the Directive, the E.U. legislator intended to ensure that personal data would flow within the Union in compliance with the fundamental freedoms of individual privacy. The Directive moves directly from its first consideration, that "the establishment and functioning of an internal market . . . require[s] not only that personal data should be able to flow freely from one Member State to another," to a second consideration, "that the fundamental rights of individuals should [also] be safeguarded."[14] The entire rulings seek to balance these two seemingly contradictory interests: (1) the free flow of personal data subject to processing; and (2) the fundamental freedoms and rights of individuals.

The Directive's goal is to promote harmonization of member states' data privacy legislation and, thereby, the free flow of data. To achieve this goal, the E.U. legislator specified a set of rules which must be implemented by the member states in their legal systems "as is," and also granted member states a margin for maneuver in such implementation. According to the principle of harmonization, member states' national legislation should be based upon the compulsory rules.

B. *Directive Inconsistency*

The Directive presents a seeming inconsistency. The Council and Commission generally pursue legislative harmonization among member states' legislation by applying a minimal approach that, while forcing member states to implement the Directive's rules domestically, leaves the states free to establish additional or more restrictive rules on the same subject. By leaving the member states free to legislate in the manner they deem most adequate, the Council seeks not only to accomplish harmonization, but also to consider national sovereignty.[15]

---

mental nature, the Council accepted the modifications and adopted the Directive on July 24, 1995.

14. Directive, *supra* note 4, at 3d "Whereas."

15. The primary objective of the Convention is to establish:

> basic principles for data protection. Each Party should take the necessary steps to give effect to this "common core" in its domestic legislation. . . . Moreover, the "common core" will result in very close harmonization between the laws of the Contracting States and hence decrease the possibility of conflicts of law or jurisdiction.

Draft Explanatory Report on the Draft Convention for the Protection of Individu-

In the case of data privacy, the Directive's criteria offer the highest coverage or protection, as compared to both consumer protection legislation and certain member states' constitutional human rights provisions.[16] According to the Council, this level of protection reflects that:

> [T]he object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; . . . for that reason, the approximation of [these] laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.[17]

The Council further states that "the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the . . . Convention."[18] Accordingly, national laws offering the highest protection would achieve two main objectives: (1) ensuring adequate protection to the right of privacy as usually ruled out by national constitutions; and (2) guaranteeing the elimination of barriers to the free flow of personal data through the harmonization of data privacy protection among member states.

Despite its decision to afford data privacy a different level of protection through the Directive, the Council has continued to leave the states free to some extent to vary the degree of protection. This, however, creates an inconsistency: flexibility and harmonization are not always compatible concepts.

This incongruity is positively stated in the Directive's ninth "Whereas," which states that:

---

als With Regard to Automatic Processing Personal Data, 19 I.L.M. 282, 299 (1980) [hereinafter Explanatory Report to Convention].

16. *See id.* at 300 (concluding, following study of Committee of Ministers, that "the present law [consisting of European Human Rights Convention and domestic law] gave insufficient protection to individual privacy and other rights and interests of individuals with regard to automated data banks").

17. Directive, *supra* note 4, at 10th "Whereas" (discussing European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221).

18. *Id.* at 11th "Whereas."

> [T]he Member States will be left a margin for manoeuver [sic] . . . [and] therefore be able to specify in their national law the general conditions governing the lawfulness of data processing . . . [I]n doing so the Member States shall strive to improve the protection currently provided by their legislation . . . within the limits of this margin for manoeuver[sic] and *in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community.*[19]

Thus, under the Directive, single member states may continue to rule independently in areas of importance.

A number of factors could lead to disharmonious national legislation. For example, national laws could diverge over the: (1) inclusion/exclusion of personal or household processing from the legal protective system; (2) protection of manual records as part of data privacy law; (3) inclusion/exclusion of legal persons among the data subjects legally safeguarded; and (4) means of balancing individual rights with legitimate business interests. These factors indicate that divergences at the E.U. level in this field could persist.

The room for discrepancy left by the Directive, however, does not seem to affect free transborder data flow among E.U. member states. The general principle stated in paragraph 2 of Article 1 prevents "Member States [from either] . . . restrict[ing or] prohibit[ing] the free flow of personal data amongst Member States for reasons connected with the protection afforded under [the Directive]."[20]

---

19. *Id.* at 9th "Whereas" (emphasis added).

20. *Id.* art. 1, para. 2. The first area of possible discrepancy is over "the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses" which the Directive states should be excluded by the application of data privacy provisions. *Id.* at 12th "Whereas" & art. 3, para. 2.

The second area of discrepancy is over manual records, which the Directive limits to cases where the data "form[s] part of a filing system or are intended to form part of a filing system." *Id.* art. 3, para. 1; *see also id.* at 10th "Whereas." The Directive defines personal data filing system or filing system as, "any structured set of personal data which are accessible according to specific criteria." *Id.* art. 2(c). As per the Directive, a manual record is subject to data privacy provisions when it is judged as a filing system "structured according to specific criteria relating to individuals, allowing easy access to the personal data in question." *Id.* at 27th "Whereas." Also, in this case, "the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State." *Id.* In any case, however, "files or sets of files . . . which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive." *Id.*

C. *Remedies*

The Directive seeks to give individuals certain remedies for actual privacy protection. One of these remedies, however, the right to block data, is problematic. Although the Directive fairly grants individuals the rights to rectify and to erase data processed in violation of the Directive, the Directive's third sanction—the right to block data—seems disproportionate. In most instances, in order to block data the whole data bank, as well as the whole processing activity, must also be blocked. This is especially true given that today's data banks are generally interconnected.

Second, the possible consequences of such an action extend far beyond the scope of both the legitimate safekeeping of individual rights and the remedies necessary to support such protection. It is difficult to contemplate violations unremediable through both the sanctions of data rectification and erasure, and somehow requiring recourse to the potentially over-reaching remedy of data blocking. In addition, the blocking of data is conceived as a remedy in cases where data is incomplete. Despite a few attempts at textual interpretation, however, the Directive's definition of incompleteness remains vague.[21]

The third area of discrepancy is over the notion of "data subject" being "an identified or identifiable *natural* person" with the consequent exclusion of the data related to *legal* persons from the scope of the Directive. *Id.* art. 2(a) (emphasis added). The European legislator, however, seems unlikely to modify the existing national "legislation concerning the protection of *legal persons* with regard to the processing of data which concern them." *Id.* at 24th "Whereas" (emphasis added). Because the legislation "is not affected by the Directive," divergence on this matter among the member states remains unsolved. *Id.*

The fourth area of discrepancy—"the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies"—is left for member states to determine, "in order to maintain a balance between the interests involved while guaranteeing effective competition." *Id.* at 30th "Whereas;" *see also id.* art. 7(f).

The fifth area of discrepancy involves whether "rights of access and information" may be imposed by member states "in the interest of the data subject or so as to protect the rights and freedoms of others." *Id.* at 42d "Whereas;" *see also id.* art. 13. For the same reason, by virtue of the provisions of Community law, member states may derogate from the provisions of the Directive concerning the right of access, the right of information and the quality of data. *Id.* at 42d & 44th "Whereas;" *see also id.* art. 13.

The sixth area of discrepancy is over the granting of "exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States" seeking to "avoid unsuitable administrative formalities, . . . [and] in cases where processing is unlikely to adversely affect the rights and freedoms of data subjects." *Id.* at 49th "Whereas;" *see also id.* art. 18, paras. 3-5. Although granting member states the opportunity to rule out few exceptions and derogations is a flexible approach that, with regard to this complex field, is proper and welcome, the same cannot be said for other points.

21. The criterion to judge the adequacy of the completeness of the data con-

In conclusion, while the Directive seeks to safeguard individual rights through permitting data rectification and erasure, the Directive goes too far by permitting data blocking. Data blocking is an excessive remedy because of its technical implications and possibly disruptive effects on a concern's entire business activity.

D. *Scope of the Directive*

The scope of the Directive's protection is delineated by three elements: (1) natural persons; (2) data identifying; and (3) data processing.

1. *Protection of Natural Persons*

The Directive protects the fundamental rights of individuals by substantiating and amplifying Convention principles. After lengthy discussion within the E.U., however, legal persons were excluded from the scope of the Directive's protection. The Directive, however, points out that it will have no effect upon existing legislation protecting legal persons with regard to data processing which concerns them.

2. *Data Which May Identify an Individual*

The Directive's protection is limited to "personal data," defined as any information concerning a natural person, identified or identifiable, even if through sounds and images.[22] The Preamble to the Directive makes the only reference to sounds and images; no mention is made in its operative provisions. As a result, there is no specific exception or guidance, of the type that a prior data subject's consent provision would provide, for personal data identification techniques such as surveillance cameras installed by banks, digitized signatures or recording systems.

a. "Sensitive" Data

Certain personal data merits higher protection because it "re-

tained in Article 6(d)'s reference to "the purposes for which [the data] were collected or for which they are further processed" is not sufficiently clear to adequately delimit this concept. *See id.* art. 6(d).

22. *Id.* art. 2(a). The Directive defines "personal data" as "any information relating to an identified or identifiable person." *Id.* 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." *Id.* Therefore, data rendered in such a way that the data subject is no longer identifiable falls outside the scope of protection. *Id.*

veal[s one's] racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership," health matters or sex life.[23] Accordingly, the Directive compels member states to prohibit the processing of such data. A few exceptions to this prohibition exist, the most notable of which rests upon the explicit consent of the data subject.[24]

b. Manual Files

With regard to the nature of records falling under data privacy protection, it is worth noting that the Convention per se excluded "manual files" from its scope.[25] The Directive, however, includes manual files in its scope,[26] although limiting applicability to data contained, or intended to be contained, in a "filing system."[27] The Directive's inclusion of manual processings has raised substantial criticism.[28] Article 3, paragraph 1, however, includes a concept of

23. *Id.* art. 8, para. 1.

24. *Id.* art. 8, para. 2. Exceptions to the general prohibition of processing are when: (1) the consent of the data subject is given; (2) it is necessary for the controller to carry his obligations and rights in the field of employment law; (3) it is necessary to protect the data subject or a third person where the subject is incapable of giving consent; (4) legitimate activities within appropriate guarantees by a non-profit body are directed solely at members and data is not disclosed to third parties without consent; (5) the data subject makes the processing public or it is necessary to do so because of a legal claim; (6) the processing is related to medical purposes; and (7) member states exercise their discretion. *Id.*

25. "The Contracting Parties undertake to apply this Convention to automated data files and automatic processing of personal data . . . ." Draft Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, 19 I.L.M. 282, 284, art. 3, para. 1 (1980). Further, the Introduction to the Explanatory Report states that "[t]he object of this Convention is . . . the legal protection of individuals with regard to automatic processing of personal information relating to them . . . . Compared with manual files, automated files have a vastly superior storage capability and offer possibilities for a much wider variety of transactions, which they can perform at high speed." Explanatory Report of Convention, *supra* note 15, at 299, intro., para. 1.

26. "[T]he protection of individuals must apply as much to automatic processing of data as to manual processing; . . . the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention." Directive, *supra* note 4, at 27th "Whereas."

27. For example, this would include "any structured set of personal data which are accessible according to specific criteria" and easily accessible as per Article 2(c). *Id.* art. 2(c). The Directive states that "nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files." *Id.* at 27th "Whereas."

28. It has been noted that the definition of "personal data filing system" is vague. The Directive defines a "personal data filing system" as "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis." *Id.* art. 2(c). Although it probably does not refer only to card index-type systems, it may refer to all correspondence files. In the latter case, the consequences in terms of administrative burdens (e.g., from notification to the Authority), problematic im-

potentiality that extends the scope of the law even further, adding an element of interpretative uncertainty as to what information is "intended to form part of a filing system."[29] Although the Directive allows member states to establish "the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set," it also emphasizes that "files or sets of files . . . which are not structured according to specific criteria, shall under no circumstances fall within [its protection]."[30]

3. *Processing Activity*

Not all personal data remains within the scope of the Directive; rather, its protection extends only to personal data subject to processing, including both automated and manual operations. Specifically, the Directive does not cover the processing of personal data: (1) concerning public security and criminal law; and (2) by a natural person in the course of a purely personal or household activity.[31]

E. *The Main Principles of Data Privacy Protection*

Three types of principles potentially promote data privacy protection. First, data privacy may be protected by establishing an independent and specialized authority, with supervising, intervening and consulting duties. Second, data privacy may be protected by a series of obligations imposed on the persons responsible for processing[32] who can then be subject to sanctions in case of a violation. Such obligations relate to: (1) information to the data subject; (2) data quality; (3) technical security; (4) notification to the Supervisory Authority; and (5) qualifying factors of processing. Combined, these five factors guarantee legitimacy of processing, protection of data and public control over processing activity.

Third, data privacy may be protected by the granting of exclusive rights to data subjects, such as the rights to: (1) be informed

plementation (e.g., from honoring the data subject's right to access, and conforming existing or new files to the new provisions of law) are significant.

29. *Id.* art. 3, para. 1.

30. *Id.* at 27th "Whereas."

31. *Id.* art. 3, para. 2.

32. The Directive refers to these persons as "controllers." *See id.* art. 2(d). A controller is defined as the individual or entity which "determines the purposes and means of the processing of personal data." *Id.* The Directive also recognized an individual or entity, known as a "processor," that "processes personal data on behalf of the controller." *Id.* art. 2(e).

(i.e., know that automated personal data exists); (2) consult the data (i.e., know the content of the information); and (3) request corrections or, in specific cases, to object to the processing (i.e., a remedy in cases of inappropriate or incorrect information). These rights allow verification of data processing for compliance with data privacy rights.

F. *The Processor's Obligations*

The Directive imposes obligations on the data controller that are connected to both the exercise of the data subject's rights and the relation of the means (i.e., specific obligations) to the scope (i.e., extent of privacy protection). In other words, the obligations are meant to fit the purpose of actually protecting the rights of data subjects. For this reason, the Directive seeks to avoid "unsuitable administrative formalities."[33] Moreover, both the Convention and the Directive determine the validity of exemptions and simplifications according to their impact upon actual data privacy protection.[34] Consequently, when exercising their discretionary powers, national legislators should make a practical and effective data privacy protection system *the* priority.

1. *Information to the Data Subject*

Legitimate personal data processing systems require data controllers to inform data subjects of a data processing related to them and also of the main features of the data collecting operations. Data controllers must do so upon collection of the data, or, if not collected directly from the data subject, upon recording the data. This obligation to provide information is subject to few exceptions.[35]

2. *Data Quality*

According to the Directive, personal data must be: (1) processed fairly and lawfully; (2) collected for specified, explicit and legitimate purposes; (3) adequate, relevant and not excessive in relation to the purposes for which they are collected; (4) accurate and, where necessary, kept up-to-date; and (5) kept in a form

33. *Id.* at 49th "Whereas."

34. *See id.* (allowing member states to provide exemption or simplification as long as processing does not adversely "affect the rights and freedoms of data subjects").

35. *See id.* art. 11, para. 2 (exempting controller from obligation to provide information when doing so "proves impossible or would involve a disproportionate effort").

which permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected.[36]

In order to be both fair and legitimate, the Directive requires that personal data processing meet one of the criteria specifically listed in Article 7.[37] The Directive, however, recognizes that the needs of different sectors will require individually tailored solutions.[38] Therefore, it encourages, mainly through the action of the member states, the establishment of codes of conduct that take into account the specific features of the various sectors.[39] These codes may be submitted to the supervisory Authority for a judgment on their conformity with the national provisions adopted pursuant to the Directive.[40]

3. *Security Measures*

Protection of data subjects' rights under the Directive requires data controllers to adopt technical and organizational measures that will ensure data "security," interpreted as protection from: (1) accidental or unlawful destruction; (2) accidental loss; (3) unauthorized alteration, disclosure or access; and (4) all other unlawful forms of processing.[41]

---

36. *Id.* art. 6.

37. *Id.* art. 7. Article 7 states that member states may provide for personal data processing only if at least one of the following criteria are met: (1) the data subject consents; (2) processing is necessary for the conclusion or execution of an agreement binding the data subject; (3) processing is necessary for compliance with the law; (4) processing is necessary to protect the vital interests of the data subject; (5) processing is necessary for the performance of a task that is carried out in the public interest; or (6) processing is necessary in the legitimate interest of the controller except when such interests are in contrast with the fundamental rights and freedoms of the data subject. *Id.* art. 7(a)-(f).

38. *Id.* art. 27, para. 1.

39. *Id.*

40. *Id.* art. 27, para. 2. Submission to the national Authority is not compulsory. *See id.* (stating that trade associations and other bodies representing other categories of controllers will "be able to submit" codes to national Authority).

41. *Id.* art. 17, para. 1. Article 17 also states that "[h]aving regard to the state of the art and the costs of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected." *Id.* The Directive's 46th "Whereas" elucidates that:

> [T]he protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing.

Id. at 46th "Whereas." The provision adds that "it is incumbent on the Member States to ensure that controllers comply with these measures." *Id.*

4. *Notification to the Authority*

In exercising its supervisory powers, the Authority relies upon the controller's notification of its intention to process personal data. In this way, the required notification ensures disclosure of the processing operation's purposes and main features. In order to avoid unnecessary administrative formalities, member states may provide exemptions from and simplification of the notification requirement.[42] At the same time, the Authority will keep a public register recording all notifications,[43] which data subjects and the public may freely access.[44]

G. *The Data Subject's Rights*

1. *Right to Be Informed*

The data subject's right to be informed flows from the controller's obligation to inform; it also substantiates the data subject's right to access data relating to him or her.

2. *Right to Access*

Through exercising the right to access, the data subject can ascertain the accuracy of data relating to her and the lawfulness of the processing. In practice, this right is exercisable because of the preliminary notification that every controller must make to the national Authority before processing personal data.[45] As a result, the Authority is a collection and distribution center for personal data information processing. The Authority completes the system of publicity by establishing a public register of the collected information. For the same reasons, the Directive also grants data subjects the right to know the logic upon which the automatic processing is based, where the exercise of this right will not adversely affect intellectual property and copyright protection software.[46]

The public register, notification to the Authority and organization of the Authority itself rely heavily upon automated means. In-

42. *Id.* art. 18, paras. 2, 4.

43. *Id.* art. 21, para. 2.

44. *See id.* (ordering that register may be examined by any member of public).

45. *See id.* art. 18 (directing controller to notify supervisory authority).

46. *Id.* art. 12 (stating that "Member States shall guarantee for every data subject the right to obtain from the controller . . . without constraint at reasonable intervals and without excessive delay or expense . . . knowledge of the logic involved in any automatic processing of data concerning him"); *id.* at 41st "Whereas" (stating that considerations referencing to intellectual property rights and copyright protecting software "must not, however, result in the data subject being refused all information").

deed, while automated means constitute the primary cause for personal privacy protection and data privacy-type of laws, they also represent an indispensable aid for implementation of these laws. The Directive opens the door for member states to limit data subjects' rights of access and information in order to protect the rights and freedoms of third parties.[47]

3. *Right to Object*

The data subject has another main right: the right to object to the processing of data relating to him or her at any time "on compelling legitimate grounds."[48] The Directive specifically states that the data subject has the right to object to the processing (apparently not on a "compelling legitimate ground" but for convenience) of personal data used in direct marketing.[49] This right encompasses the related data subject's right "not to be subject to a decision which produces legal effects concerning him" and "which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him."[50]

4. *The Data Subject's Consent*

In certain circumstances, the controller of data must obtain the data subject's consent prior to processing or obtaining personal data. The Directive defines consent as "any freely given specific and informed indication of [the data subject's] wishes by which the data subject signifies his agreement to the personal data relating to him being processed."[51] But the Directive qualifies "consent" differently elsewhere in the text. Namely, according to the circumstances, it may have to be unambiguous[52] or explicit.[53]

Some commentators have expressed a concern that requiring *unambiguous* consent could contradict certain "opt out" procedures currently practiced in a few member states. Under opt out procedures, data subjects are fully informed and given an opportunity to object to the processing or transferring data relating to them.

47. *Id.* art. 13, para. 1. Article 13 states that restrictions and exemptions to the rights to access and information, among other rights, are allowed when the restrictions and exemptions constitute a necessary measure to safeguard: (1) national security; (2) defense; (3) public security; or (4) prevention, investigation and prosecution of criminal offenses. *Id.*

48. *Id.* art. 14(a).

49. *Id.* art. 14(b).

50. *Id.* art. 15, para. 1.

51. *Id.* art. 2(h).

52. *Id.* arts. 7, 26.

53. *Id.* art. 8.

H. *The Authority*

A supervisory Authority ensures compliance with the Directive's principles and regulations. This Authority is an independent body, able to investigate, intervene on behalf of and promote legal actions. When the data subject seeks to challenge the decisions of the Authority or pursue an alleged violation of the right to privacy by third parties, the data subject may always seek recourse in an ordinary jurisdiction.

I. *Transborder Data Flow*

The Directive explicitly states that, once its provisions have been adopted, member states "shall neither restrict nor prohibit the free flow of personal data" among member states for reasons connected with the protection of the rights and freedoms of natural persons.[54] The Directive prohibits the transfer of personal data to non-member states not offering adequate personal data protection.[55] The receiving state's protection is adequate only if it is equal to or higher than that granted to the same data by the origin state.[56] When assessing a third country's protection, the Authority considers all the circumstances surrounding a data transfer, the rules of law in force in the third country in question, as well as the professional rules and security measures.[57] The Convention and Directive both state this policy of reciprocity, rather than a more onerous one of license to export, to avoid potentially harmful auto-

54. *Id.* art. 1, para. 2.

55. *See id.* art. 25, para. 4 (indicating that if "a third country does not ensure an adequate level of protection . . . , Member States shall take the measures necessary to prevent any transfer of data").

56. *Id.* art. 25, para. 2. This provision specifies that "[t]he adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of transfer operations." *Id.* The provision adds that:

> [P]articular consideration shall be given to the nature of the data, the purpose and the duration of the proposed processing operation or operations, the country of origin and the 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 those countries.

Id. This guidance on the meaning of "adequate level of protection" seems to address the concerns raised by some European Associations. In particular, these associations feared that once the Directive was introduced in the member states, the Directive's level of protection would become the benchmark for adequacy, impeding data flow to jurisdictions not having formal data protection legislation. This concern related mainly to the United States and Japan, which do not have extensive legislation in the field.

57. *Id.* art. 25, para. 2.

matic processing in different countries.[58] Under the Directive, therefore, reciprocity is the only prerequisite for the legitimate transfer of personal data over E.U. borders.

In certain instances, the Directive provides exceptions to the reciprocity requirement.[59] For example, an exception applies to data transfers where the parties have a contract necessitating transborder personal data flow. The transfer of data among companies pertaining to the same group, however, does not fall within any of these exceptions. Consequently, in order for a company subject to the Directive to continue the personal data transfer with a non-E.U. affiliate, one of the exceptions exclusively listed in the Directive must apply (e.g., the adoption by both parties of specific measures, such as adequate contractual provisions, to remedy the insufficient protection in the third country).

On the whole, the Directive's exceptions do not address a number of important issues related to the activity of information technology and telecommunication service providers. In the context of electronic mail, the service provider and receiver of a

58. A still true excerpt from the Convention states that:

> [It] should make no difference for data users or data subjects whether data processing operations take place in one or in several countries. The same fundamental rules should apply and data subjects should be given the same safeguards for the protection of their rights and interests.
>
> In practice, however, data protection grows weaker when the geographic scope is widened. Concern has been expressed that data users might seek to avoid data protection controls by moving their operations, in whole or in part, to "data havens," i.e., countries which have less strict data protection laws, or none at all.

Explanatory Report of Convention, *supra* note 15, at 300, intro., para. 9.

59. According to Article 26 of the Directive, the transfer of personal data to a non-member state that has an inadequate level of protection may take place, by way of derogation from Article 25, only if:

> (a) the data subject has given his consent unambiguously to the proposed transfer; or
>
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
>
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
>
> (d) the transfer is necessary . . . on important public interest grounds, or for the establishment, exercise or defense of legal claims; or
>
> (e) the transfer is necessary in order to protect the vital interests of the data subject; or
>
> (f) the transfer 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, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

Directive, *supra* note 4, art. 26, para. 1.

message are unlikely to have a contractual relationship.[60] Similarly, in such a circumstance, it may be impossible or, at the least very difficult, to obtain the data subject's consent to the transfer, another of the listed exceptions to the prohibition of transborder data flow when reciprocity is missing.[61]

Application of the Directive in other contexts—such as the operations of bank payments, credit card transactions, travel reservations and even the Global Information Infrastructure—could lead to the same problems. Notably, however, the E.U. Commission may verify that a third country's protection is adequate; in which case, the member states must then adopt proper measures in compliance with the Commission's decision.

J. *Judicial Remedies, Liability and Penalties*

Every person is entitled to a judicial remedy and possible prior recourse before their national supervisory Authority for any violation of personal data privacy rights conferred by national law.[62] If the individual suffers damages as a result of an unlawful processing of personal data, he or she can receive compensation from the controller.[63] The Directive requires member states to adopt suitable sanctions for infringement of laws adopted pursuant to its provisions.[64]

IV. CONCLUSION

Europe's experience relating to data privacy matters during the last fifteen years or so—especially as it relates to the creation of the Directive on personal data privacy protection—indicates that, in order to adequately safeguard data privacy rights, certain important issues must be fully resolved. First, there is a continuing need for an overarching data privacy protection law. Second, there is the need for a system that successfully balances the rights to privacy, freedom of information, economic and social progress, and trade

60. *See id.* art. 26, para. 1(b), (c) (requiring contractual relationship for exception to apply). It is also questionable that paragraph 1(c) covers the example referred to in the text. *See id.* art. 26, para. 1(c).

61. *Id.* art. 26, para. 1(a) (requiring, as case of derogation from Article 25, that "the data subject has given his consent unambiguously to the proposed transfer").

62. *Id.* art. 22.

63. *Id.* art. 23, para. 1. The controller can escape liability if he can demonstrate that he is not at fault for the event that caused the claimant damage. *Id.* art. 23, para. 2.

64. *Id.* art. 24.

expansion. Third, there is the need for actual protection of data privacy rights by a protection system that is not financially and administratively convoluted or onerous. Finally, there remains the need for coordination and harmonization among states, third countries and other international institutions on how to handle data privacy issues.