Michigan Journal of International Law

Volume 5 | Issue 1

1984

The Council of Europe Convention of the OECD Guidelines on Data Protection

Jon Bing
University of Oslo

The Council of Europe Convention and the OECD Guidelines on Data Protection

Jon Bing*

INTRODUCTION

Modern computer industries and computer services have many international effects. This was perhaps not obvious a couple of decades ago when computers were big, cumbersome machines which fed on punched cards and belched out piles of paper. But it is glaringly obvious today, the result of advances in telecommunication technology and the growth of computer networks. Given this international nature of data processing, the political and legal concerns have also become international.

Data protection [1] has been a major concern since the late 1960s. The first general data protection statute was enacted by the West German state of Hesse in 1970, [2] and the first national statute by Sweden in 1973. [3] Other European countries followed their example, [4] and in North America both the United States and Canada developed general and quite extensive data protection legislation. [5]

It became apparent to those concerned with data protection, however, that it could not be achieved solely through national legislation. The efforts of an international organization which could coordinate and organize the drafting of international legal instruments were required. Arguably, no really adequate organization existed. Organizations mainly concerned with telecommunications, like the International Telecommunications Union (ITU), had no tradition of tackling issues of a political and social nature such as data protection. The two organizations which initiated transnational legal instruments in the data protection field were the Council of Europe and the Organization for Economic Cooperation and Development

* Jon Bing, Dr. Juris, is Associate Professor at the Norwegian Research Center for Computers and Law, a Department of the Faculty of Law at the University of Oslo. He is currently Chairman of the Committee of Legal Data Processing, Council of Europe, and has wide research interests in the area of computers and law.

(OECD). These organizations are well suited to tackle legal issues related to national policies or international trade, although not equipped to discuss technical standards or other problems directly related to telecommunications technology. The Council of Europe and the OECD approached the issue from very different perspectives, reflecting the different purposes of the two organizations.

The Council of Europe has traditionally been a human rights organization, although it has moved into such other areas as social welfare and penal legislation.[6] The organization even has a Committee on Legal Data Processing, which is mainly concerned with legal information services.[7] The OECD, as its name implies, is principally interested in trade and the economic aspects of cooperation between member countries.[8] The organizations also have a different membership. The Council of Europe is a regional organization for Europe (including Turkey), while the OECD is sometimes referred to as a "club of rich countries" including, in addition to its European membership, the United States, Canada, Australia, and Japan.

The first international legal instruments to be adopted were two Council of Europe resolutions in 1973 and 1974, the first on "the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector,"[9] and the second on "the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector."[10] The more comprehensive "Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data"[11] (Convention) was adopted in 1980. As of November 15, 1982 thirteen countries had signed the Convention (Austria, Belgium, Denmark, Federal Republic of Germany, France, Iceland, Luxembourg, Norway, Portugal, Spain, Sweden, Turkey, and the United Kingdom). Of these only Sweden has ratified the Convention (September 29, 1982), and it will not enter into force until five countries have done so (art. 22(2)).

The OECD established its first expert group, the Data Bank Panel, as early as 1969. In 1978, a new Group of Experts on Transborder Data Barriers and Privacy Protection was established and instructed to draft a set of recommendations.[12] The resulting "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"[13] (Guidelines) were adopted by the OECD in 1980.

It would be expected, given the different natures of the two organizations which drafted them, that the two instruments would differ, the Convention focusing on the human rights aspects of the traditional privacy concept, and the Guidelines focusing on data protection and its impact on international trade and economic cooperation.[14] There are, however, remarkable similarities in the orientation of the two instruments.[15] Each

clearly recognizes as a basic issue the conflict between the ideal of data protection and the ideal of free flow of information between countries.[16]

This article will not, however, analyze the two instruments in light of the differing natures of the organizations which produced them. Instead it will describe and compare the rules of data protection as they emerge in the instruments. Although this will require some assessment, the main objective will be to explain and amplify.

SCOPE AND BASIC CONCEPTS

Before analyzing the substantive norms, the scope of the two instruments will be examined. The scope is described by the Convention in article 3 and the Guidelines in paragraphs 2-6. Both instruments seek to protect "personal data," which is defined *identically* in the Convention article 2(a) and in the Guidelines paragraph 1(b) as "any information relating to an identified or identifiable individual."[17]

The Guidelines are based wholly on this basic concept of personal data, while the Convention introduces a definition of an "automated data file," which is a "set of data undergoing automatic processing" (art. 2(b)). In this the Convention resembles most national data protection legislation, in which substantive rules are related to some sort of definition of a "personal data system."[18]

The difference between the Convention and the Guidelines should not, however, be exaggerated. The Guidelines also presume some structuring of the data; they do not apply to single data elements.[19] This difference between the two instruments indicates one of the basic choices in determining the scope of a data protection agreement: whether to include manual or non-automated systems. The Guidelines apply generally to "personal data," with some vaguely stated qualifications of nature and context (para. 2). Peter Seipel, one of the major architects of the Guidelines, points out that there was "an unwillingness to use any terms which might suggest that automated processing is involved; thus even the word 'file' is banned from the text."[20] The Guidelines, therefore, are not restricted to computerized systems. This classification corresponds to the position of the computer industry, which although appreciating the importance of the data protection issue, maintained that it was unjustifiable to limit it to computerized systems.[21] However, the Guidelines explicitly state that they should not be interpreted as preventing their application solely "to automatic processing" (para. 3(c)).

The Convention explicitly applies to "automated personal data files" (art. 3(1)) although, again a state may give notice that it will also apply the Convention to "personal data files which are not processed automatically"

(art. 3(2)(c)). Thus, although the two instruments differ in their initial positions, they will both accomodate the extension of their principles to manual systems, or restriction to computerized systems. There may still be a difference resulting from the Convention's in principle applying only to "files," while the Guidelines also apply to "data," even when not structured in files. But as discussed above, the consequences of this difference may not be great.[22]

Another major issue involving the scope of the instruments was whether the data of *legal persons* should be protected. (Some countries, including Denmark and Norway, have extended their data protection legislation to legal persons.[23]) Both instruments are initially restricted to the data protection of physical persons, but permit the extension to legal persons. The Convention does this explicitly, stating that a state may give notice that it will apply the Convention to "information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies posess legal personality" (art. 3(2)(b)). The Guidelines allude to their extension to legal persons more obliquely. Paragraph 3 suggests that the Guidelines should be applied flexibly.[24] Although the paragraph contains no explicit reference to legal persons, the Explanatory Memorandum states "protection may be afforded to data relating to groups and similar entities whereas such protection is completely nonexistent in another country."[25]

This difference in the two instruments may be explained in two ways. First, the common law countries[26] play a more dominant role in the OECD than in the Council of Europe, and in these countries it is less obvious that data protection may be associated with an entity which is not a physical person. This may be especially true in the United States, where the rights of privacy are largely derived from the constitutional rights of an individual. Another possible explanation is that the OECD embarked on a new study immediately following the study resulting in the Guidelines, which was to concentrate on *non-personal* data traffic, and an important category within this heterogeneous group would be data on legal persons.[27] Whatever the explanation for the different methods of accomodating an extension to non-legal persons, from the point of view of a member state the scope is the same. On a less controversial point, both instruments also apply to data in the public and private sectors (Convention, art. 3(1); Guidelines, para. 2). The Guidelines specifically mention that they may be affected by the division of powers in a federal country (para. 5).

Finally, both instruments allow exceptions to their data protection requirements for certain limited reasons. The Convention permits a Party to derogate from certain provisions in the interest of "state security, public safety, the monetary interests of the State or suppression of criminal offenders," (art. 9(2)(a)) and mentions "protecting the data subjects or the

rights and freedoms of others" (art. 9(2)(b)). The Guidelines also explicitly mention exceptions based on "national sovereignty, national security and public policy (*ordre publique*)" (para. 4). In addition, due to the binding nature of the Guidelines, member countries may take other exceptions, although these must be limited in number and made public (para. 4(a) and (b)).

ANALYSIS OF SUBSTANTIVE PRINCIPLES

Introduction: Data Protection

In order to analyze the two instruments, some sort of comparative methodology is necessary. The ideal methodology would begin with a clear and agreed definition of "data protection." Unfortunately, however, no real consensus of a definition—or even a characterization—exists. While neither instrument defines data protection, both instruments obviously have an understanding of "data protection" reaching beyond "privacy" in the narrow sense of protecting private or intimate information. The difficulty in agreeing upon a definition again may be partially attributable to differences between common law and Continental European doctrines. However, it has been pointed out that this is not the whole explanation; the different experiences of the various member countries in actually regulating the use of personal data have been important.[28]

Because of this impossibility of a precise definition in the international literature on data protection, this article's analysis is based on a system developed by the research program on information law of the Norwegian Research Center for Computers and Law (The Norwegian Center).[29] This system of analysis is based on a *decision-oriented view* of data protection, in contrast to the privacy orientation of the conventional concept. The system defines data protection as the protection of various interests which the individual has in the uses made of his personal data in decisions which may have an effect on him. If there is a strong possibility that a decision will have such an effect, the data protection interests are correspondingly strong.

For the purposes of this article, three interests will be scrutinized. First, an individual has an interest in having adequate personal data about him available to a decision maker for the latter to reach an appropriate decision. This implies his interest in having all relevant data available, and in having all irrelevant, misleading or dated data excluded. Obviously controversy often will center on the relevancy and accuracy of personal data. The Norwegian Center uses the term "completeness" for this interest.[30] This term does not, perhaps, sufficiently indicate the strong linking between the individual's interest and the decision and its purpose, and the term

"adequacy" would seem to be more appropriate. Second, individuals have an interest in confidentiality, because of their reluctance to have personal information communicated to a wider circle than is absolutely necessary. Third, individuals have an interest in openness, which is the interest in knowing what personal data is used for what purposes by which organizations. Requiring openness is a prerequisite for enforcing the first two interests. Each of these three interests will be discussed in further detail below.

The Interest in Adequacy

The interest in adequacy exists in decision situations in which personal data is relevent. The data subject is interested in having *all* relevant data known to the decision maker in an adequate form. There are obvious problems in implementing this principle: for example, who is to decide whether certain data is relevant? Because of such problems, the interest of adequacy is generally found only partially implemented in the form of what is usually known as the principle of relevancy:[31] personal data should be relevant to the business of the controller of the file, and the data used should be correct and not misleading.

The Convention opts for the principle of relevancy, which is to be implemented by requiring that the data should be related to "specified and legitimate purposes"; "adequate, relevant and not excessive" in relation to these purposes; and finally, "accurate and, where necessary kept up-to-date" (art. 5(b)-(d)). A very similar construction is found in the Guidelines. Here too the principle is founded upon the premise that the "data should be relevant to the purposes for which they are used" (para. 8). These purposes should be specified "not later than the time of data collection," and subsequent use should be limited to these original purposes, or "such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose" (para. 9). The data should be "accurate, complete" and if necessary "kept up to date" (para. 8).

In both instruments this basic principle of relevance is called the principle of "data quality," and it is implemented in much the same way. There is some difference in the formulation of the concept; for instance, in the Guidelines the data only has to be accurate when dictated by some specified purposes (para. 8), while under the Convention data should always be accurate (art. 5(d)). But a more important similarity is the fact that the data must be relevant to the explicit purpose of a controller. Outside of this purpose, data cannot be collected or stored without violating the data protection rights of the individual.

According to the decision-oriented view of data protection, the interest in adequacy is perhaps the most important. However, in implementing this principle two major limitations of the rights of the data subject were

introduced. First, as discussed above, in both instruments the principle of adequacy was reduced to a "principle of relevancy," which does not require that all relevent data elements be included, but rather that those included be relevant.

The second limitation is less obvious, but potentially of greater consequence to the rights of the individual. The Guidelines require that the data must be relevent to purposes stated by the controller, but with no limitations to what kind of purposes may be legitimately stated (para. 9). The Convention, on the other hand, requires that the stated purpose must be "legitimate," a qualification which seems to imply that not *any* stated purpose will do, but rather that it must be related to the business or general purpose of the activities of the controller (art. 5(b)).[32]

The Interest in Confidentiality

The interest in confidentiality is the interest in not having personal data disseminated in wider circles than necessary. The data subject understandably wishes to control the communication of his personal data. This interest exists outside the area of data protection law; for example, in the traditional confidentiality of communications with medical doctors or priests.

Data protection law introduces, however, supplemental principles. One of them, found in both the Convention and the Guidelines, is the "collection limitation principle," which is stated more strongly in the Guidelines: "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject" (para. 7). This paragraph combines the principle of "lawful collection," the principle of consent by the data subject and the principle that there should be some limits to the collection of personal data, which means that no general license should be given, not even to certain public agencies. The Convention has the same principle, but in a weaker version, including only the principle of "lawful collection" (art. 5(a)).

Other limitations are contained in the instruments. The Convention, as do many national data protection acts,[33] limits the collection of *sensitive data, i.e.,* data closely associated with the private life of an individual, or which may have defamatory power (art. 6). The Convention specifies six categories of sensitive data: (1) data revealing racial origin; (2) data revealing political opinions; (3) data revealing religious or other beliefs; (4) data concerning health; (5) data concerning sexual life; (6) data relating to criminal convictions.[34] These sensitive data receive special protection in that they may not be "processed automatically unless domestic law provides appropriate safeguards" (art. 6). Although this protection is rather

vague, it obviously directs member countries to take extra measures with computerized systems handling this sort of data.

The Guidelines do not include explicit principles regarding sensitive data. The reason may be the difficulty of deciding what data really are sensitive, as the assessment would differ depending on the political system, the traditions and general sentiment of a culture or a country. The Explanatory Memorandum, addressing the collection limitation principle, discusses this point:

> It could be argued that it is both possible and desirable to enumerate types or categories of data which are *per se* sensitive and the collection of which should be restricted or even prohibited. There are precedents in European legislation to this effect (race, religious beliefs, criminal record, for example). On the other hand, it may be held that no data is intrinsically "private" or "sensitive" but may become so in view of its context and use. This view is reflected, for example, in the privacy legislation of the USA.[35]

Although the Guidelines do not explicitly give any special protection to sensitive data, considerations related to sensitive data issues influenced the collective limitation principles and the scope of the Guidelines. As discussed above, they apply to personal data which pose a danger to privacy and individual liberties, including dangers due to the "nature or the context" in which the data are used. The Guidelines also do not hinder the effectiveness of sensitive and non-sensitive data classification found in national laws.[36]

The confidentiality limitations discussed to this point have described limits on the *collection* of personal data. Obviously there is another side to the confidentiality interest, which is limitation on the dissemination from a controller who has gained lawful access to personal data. The Guidelines regulate the dissemination of data through the "use limitation principle" (para. 10). Personal data may only be communicated to a third party according to the specified purpose of the controller. As mentioned above, this purpose should be stated prior to the collection, and where appropriate, the data subject should be informed of the purpose or give his consent to the collection (paras. 8 and 7). This system introduces a strong regime controlling dissemination. There are, however, two exceptions to this rule (paras. 10(a) and (b)). First, if the data subject consents, data may be communicated to parties not embraced by the original purpose of the controller. This is obviously an extention of the principle of "informed consent," and as the data subject is in control, it presents no data protection problem. The second exception refers to data required by the "authority of the law," which is obviously a necessary exception. The state may, for

example, demand certain information from employers for tax control purposes.[37]

Interestingly, the Convention does not include any explicit principle limiting the dissemination of data, although an implicit limitation may be derived from article 5(b), which states that data should not be used in a way incompatible with the specified and legitimate purposes of the controller. As paragraph 10 in the Guidelines only articulates what is already implied by the original purpose limitations, arguably the same limitations follow from the Convention. Furthermore, it may be that the practical results of the Guidelines' emphasis upon control of the data subject, both in collection and dissemination, in comparison to the Convention's emphasis that the purpose of the controller must be *legitimate*, deriving the limitation to dissemination from this qualification, are very similar. It would indeed be difficult to find examples of dissemination permitted by the Convention, but prohibited by the Guidelines, even if the Convention does not explicitly regulate dissemination.

In between the collection and dissemination of data is its storage. In principle storage is of minimal interest in data protection legislation, with the exception of *unauthorized access or dissemination.* This obviously will be a violation of the data protection rights of the data subject, bringing data out of the control of the legitimate controller and the data subject alike. In the Convention there is a principle of *anonymization.* Personal data should not be stored in a form permitting identification "longer than is required for the purpose for which those data are stored" (art. 5(e)). Though the Guidelines lack an explicit principle of this nature, the Explanatory Memorandum argues that the purpose specification principle may make it necessary "to have [the data] destroyed (erased) or given an anonymous form."[38]

Both instruments also refer to *data security,* as does most national legislation.[39] The Convention states that "appropriate security measures" should be taken against "accidental or unauthorized destruction or accidential loss as well as unauthorized access, alteration or dissemination" (art. 7). The Guidelines state that "reasonable security safeguards" should be taken against "such risks as loss or unauthorized access, destruction, use, modification or disclosure" (para. 11). The wording is slightly different, but the principle seems identical. No absolute standard of data security is imposed since the appropriate standard would depend upon the risks involved. Therefore, the instruments require the taking of "appropriate" or "reasonable" security measures. The instruments explicitly apply not only to unauthorized penetration of the system but to accidental distortion as well.

In summary, as with the interest in adequacy discussed above, the stated purpose of the controller plays a critical role in the instruments' protection of the interest in confidentiality. The limitations on collection and dissemination are derived from the stated purpose of the controller, with only

minor differences between the two instruments, supplemented by a rather general provision on data security.

The Interest in Openness

In order to enforce the interests and rights discussed above, the data subject must have sufficient information about the collection, use and dissemination of his personal data. The individual's right of access to his own file has been dubbed the "magna carta of the computer age." Without resorting to such familiar clichés, openness is nevertheless a crucial part of the structures of the two instruments, as it is in national data protection legislation.[40]

The Guidelines introduce a rather general principle of openness, stating that there should be "a general policy of openness about developments, practices and policies with respect to personal data" (para. 12). The Guidelines (paras. 12 and 13) and the Convention (art. 8) specify how this is to be achieved.

The first concern of the data subject would be to identify where his data are used. Both instruments include the principle that means should be available to "establish the existence and nature of personal data" (Guidelines, para. 12), or "the existence of an automated personal data file" (Convention, art. 8(a)). The basic differences between the two instruments result in a slightly differing phrasing of the principle in each instrument, but they are substantially the same. Once the existence of data is established, the data subject would next want to know the purpose of the controller's use. Both instruments permit this (Guidelines, para. 12 and Convention, art. 8(a)). As it has been established in the discussion above that purpose plays a crucial part in the operation of the other substantive data protection principles, it is rather surprising that both instruments grant to the data subject only the right to be informed of the "main purposes" of the system. The restricted nature of this right is not completely reconcilable with the importance placed on purposes, rather than *main* purposes, in the general design of the instruments.

Finally, the data subject should be able to obtain the identity and address of the data controller.[41] This information permits the data subject to exercise his explicit right to be informed whether the data relating to him are held by the controller (Guidelines, para. 13(a); Convention, art. 8(b)). If such data exists, the data subject may then request that this data be communicated to him. Both instruments require that this information must be communicated without excessive delay; and at a charge, if any, that is not excessive (Convention, art. 8(b)); Guidelines, para. 13(b)(i)-(iv)). Under the Convention, these requirements only apply to the controller's response as to whether data relating to the subject are stored, not to the

communication of the actual data. In this important detail, the interests of the data subjects are better served by the Guidelines.

Both instruments additionally require that the data should be communicated in an intelligible form. The Guidelines further specify that the data should be communicated in a "reasonable manner" (para. 13 (b)(ii)). This does not seem to carry much independent meaning, and is not commented upon in the Explanatory Memorandum.

After receiving the data, the data subject has the right to challenge its validity (Convention, art. 8(c)); Guidelines, para. 13(d)). Through this challenge, the data subject may require rectification or erasure of data which does not comply with the substantive principles set out in the instruments. There is an interesting variation of wording in the instruments. The Convention states simply that the data subject may obtain "rectification or erasure," while the Guidelines state that he may have the data "erased, rectified, completed or amended." The reason for this difference may be that the Guidelines recognize that an absolute right of erasure or rectification would pose many practical problems in certain instances. For example, if invalid information from a data file was published by a newspaper, a data subject should not be able to require the controller to erase the news item containing misleading personal data. Instead, an explanation as a correction to the item should be added. This would then constitute a "completion" or an "amendment" rather than an "erasure" or "rectification."

An even more basic right supplements the right to challenge the data communicated. It is the right to challenge the controller's refusal to confirm whether data relating to the data subject are stored by his operation (Convention, art. 8(d); Guidelines, para. 13(c)).

The Convention permits countries to make exceptions to the principle of openness (art. 9). As mentioned above, exceptions can be made to protect national security interests.[42] Exceptions may also be made in respect to the rights established under articles 8(b), (c) and (d) in connection with "automated personal data files used for statistics or for scientific research purposes" (art. 9(3)). This last exception is consistent with the basic principles of data protection. Such files are not used to make decisions about individuals, although they may be pertinent to larger groups of persons. Therefore the data protection interests of the data subject are not pronounced. Also, access to individual files in these cases may cause administrative headaches and be very expensive. Some national legislation has consequently excluded these systems from the principle of openness,[43] and the Convention accomodates these countries by making an exception possible.

The Controller

In order to make the substantive principles operative, the instruments not only give rights to data subjects, but also impose obligations on the "controller." The Guidelines define the controller as "a party who, according to domestic law, is competent to decide about the contents and use of personal data, regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf" (para. 1(a)). According to the Convention, the "controller of the file" is "the natural or legal person, public authority, agency or any other body who is competent according to his national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which processes should by applied to them" (art. 2(d)). The definitions seem to identify the same person, although the OECD definition has to be somewhat broader, because it includes controllers responsible for data not organized in "files."

The Guidelines introduce the "accountability principle," which states that the controller should be responsible for implementing the "Basic Principles of National Application" contained in Part Two (para. 14). The Convention states that the member country should give the data subject a remedy for his requests that are consistent with the principle of openness and the other substantive principles, if these requests are not complied with by the controller (art. 8(d)). Therefore, both instruments have made the controller responsible for achieving the obligations of the substantive principles, and sanctions under national law may be requested against a controller not fulfilling his duties according to the instruments (Convention, art. 10; Guidelines, para. 19(d)).

Transborder Flow of Data

Because the Convention and the Guidelines are both international legal instruments, one would expect to find a number of provisions dealing with international aspects of data flow. However, compared with the substantive protection provisions, the provisions on transborder data flow are quite brief.

When European data protection legislation emerged, and the concern over possible abuses of privacy rights in connection with transborder data flow was first voiced in the early 1970s, some United States critics saw this as a protective measure. Behind the claim of "data protection," it was argued, the European countries were erecting barriers to protect their markets from the large United States suppliers of computer services. It is indeed difficult to assess the activities of the Council of Europe and the OECD without appreciating that the debates on the Convention, and, even

more so on the Guidelines, also were discussions of the future information market. In light of this background, it is quite important that both instruments state that data protection legislation should not be used for protectionistic purposes.

The Convention states that a party to the Convention shall not "for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party" (art. 12(2)). The Guidelines refer to this problem in the Preamble, and restate the principle in the text: "(m)ember countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder data flows of personal data that would exceed the requirements for such protection" (para. 18). The Explanatory Memorandum expands on this provision, stating that the principle is not intended to limit the rights of member countries "to regulate transborder flows of personal data in areas relating to free trade, tariffs, employment and related economic conditions for international data traffic. These are matters which were not addressed by the expert group, as they are outside its mandate."[44]

Though quite modest in their wording, both instruments clearly state that data protection legislation shall not be used as an instrument to regulate the marketplace of information services. Equally clearly, they do not specify what type of regulation of the marketplace may be desirable or appropriate.[45] In addition, the Guidelines require member countries to take "all reasonable and appropriate steps" to ensure that transborder data flows, including transit of data through a country, are "uninterrupted and secure" (para. 16). This principle could be seen as mainly concerned with technical issues, which might be better left for the ITU or similar organizations to discuss. One should remember, however, that the Guidelines are not limited to flows through computer or telecommunication networks. Therefore, it may be quite appropriate in this very general instrument to state this important principle.[46]

The instruments provide two exceptions to the principle that data protection should not be used to erect barriers to transborder data flows. The first exception deals with *data havens* and similar strategies to avoid the data protection measures of a country. Both instruments allow a country to restrict transnational data flows to and from a country which does not observe the provisions in the instruments (Convention, art. 12(3); Guidelines, para. 17). The Guidelines also have a general provision in which the member countries are asked to respect each other's interest in data protection (para. 15).

The second exception permits different levels of data protection in different countries, especially for sensitive data which may be defined differently in different national acts. Both instruments state that the "na-

ture" of the data is one permissible reason for imposing restrictions on the transborder flows when the prospective importing country does not have "equivalent protection" (Convention, art. 12(3)(b); Guidelines, para. 17). The word "nature" obviously includes sensitivity grading. The Convention also mentions "categories of automated personal data files," which may mark a difference between the two instruments. However, arguably the inclusion in an "automated data file" of personal data is a matter of their "nature," and therefore this may allow a permissible exception under paragraph 17 if the other country does not offer an equivalent protection to such files.[47]

The more important principle, perhaps, is the implied corollary of the provisions. If an equivalent protection is offered by another country, the free flow of personal data across that border should be ensured. For this reason, there is an advantage in joining both the Convention and the Guidelines. By respecting the substantive principles of data protection set out in the instruments, one is granted a place in the growing international marketplace of information services. This seems to be the main reason the United Kingdom signed the Convention.[48]

One problem remains unsolved by both instruments: the problem of choice of law. This problem was discussed by both international organizations, but with no satisfactory solution.[49] The only reference to the issue is found in the Guidelines, in which member countries agree to work towards the development of principles to govern the applicable law in cases of transborder data traffic (para. 22).

National Implementation

As discussed above,[50] when the Convention enters into force (when five member countries have ratified it, art. 22), its provisions become legally binding for the country in question. Whether the provisions would have to be introduced into the national system by an act of transformation would depend on that legal system, but the state has an obligation to make the provisions or corresponding norms part of its legal system. In this way, the nature of a convention ensures its introduction into national law.

The Guidelines, on the other hand, are not legally binding, as their name suggests. Therefore their provisions may be phrased with less thought to the detailed national implementation. This basic difference should be borne in mind when comparing and interpreting the two instruments. Nevertheless, the members of the OECD consider the Guidelines to be practically binding, demonstrated by their adoption with reservations by certain countries—an act which might otherwise be thought superfluous for a non-binding instrument. The Guidelines catalog different ways in which the provisions may be implemented, corresponding roughly to the

different strategies which have been pursued by member countries (para. 19).

International Cooperation

Both instruments also include provisions for international cooperation. The Convention has a chapter on mutual assistance (arts. 13-17). Each party names one or more authorities who will play a special role in mutual assistance; for those countries which have created a data protection authority (art. 13(2)), this authority will certainly be the one designated. On request, such an authority will assist in pursuing the goals of the Convention. Also, the parties take upon themselves the obligation to assist data subjects who reside abroad (art. 14(1)).

This system of mutual assistance provides an adequate extraterritorial extension of data protection, bypassing some of the technical difficulties for such an extraterritorial exercise of power. In the long run, this system of mutual assistance could prove valuable and useful.

The Guidelines have more general provisions facilitating the exchange of information on national data protection measures (para. 20). Member states should also establish "procedures" for information exchange and mutual assistance (para. 21). The nature of this "machinery of cooperation" however, is not specified.[51]

The Convention calls for the establishment of a "consultative committee" (arts. 18-20). This committee may play an important role in the development of the Convention and associated international instruments. However it will not be formed until the Convention enters into force, and by then some other mechanisms for international cooperation may be too well established for the committee to assume a leading role. The data protection authorities already have established a routine of annual meetings, in which common policy issues are discussed, and where a considerable amount of information exchange and cooperation takes place.

CONCLUSION

It would be precarious indeed to state a general conclusion after this introduction to the Council of Europe Convention and the OECD Guidelines. It is obvious, after this examination, that the two instruments generally correspond, as would be expected due to the contemporaneousness of their draftings, and the overlap between the delegations. The fact that the Council of Europe is essentially a human rights, and the OECD essentially a trade, organization is not very apparent in the instruments, and this, perhaps, is some sort of conclusion in itself. It should also be emphasized

that the different legal nature of the two instruments makes it impossible truly to compare them. Because the Guidelines are not legally binding, member countries may interpret their provisions more liberally than the provisions in the Convention. The possible implications of this fact are still not clear.

More importantly, these instruments should be seen as the first examples of the international regulation of the information market. Both instruments explicitly state that they are not initially intended to regulate trade. But since information services to a large extent include personal data, the instruments will obviously have an impact in this area.

The instruments also herald future regulation. The OECD is presently working on "non-personal" data flows. If and when this work is completed, the two hemispheres of data will unite and form an overlapping global regulatory framework. This framework will be essential for the development of the information market, which is one of the fastest growing economic sectors of international trade. The importance of this work cannot be underestimated, and in this work the Council of Europe Convention and OECD Guidelines are pioneering efforts.

COUNCIL OF EUROPE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

Final Draft Approved By European Committee On Legal Cooperation, 27 June 1980 And Presented To Council Of Ministers For Adoption

Preamble

The Member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its Members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms.

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing,

Reaffirming at the same time their commitment to freedom of information regardless of frontiers,

Recognizing that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

Chapter I—General Provisions

Article 1—Object and purpose

The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection').

Article 2—Definitions

For the purpose of this Convention:

a) 'personal data' means any information relating to an identified or identifiable individual ('data subject');

b) 'automated data file' means any set of data undergoing automatic processing;

c) 'automatic processing' includes the following operations if carried out in whole or in part by automated means: storage of data; carrying out of logical and/or arithmetical operations on those data; their alteration, erasure, retrieval or dissemination;

d) 'controller of the file' means the natural or legal person, public authority, agency or any other body who is competent according to his national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which processes should be applied to them.

Article 3—Scope

1. The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

a) that it will not apply this Convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject in its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions in its domestic law;

b) that it will apply this Convention also to information relating to groups of persons, associations, foundations, companies, corporations and

any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

c) that it will apply this Convention also to personal data files which are not processed automatically.

3. Any State which has extended the scope of the Convention by any of the declarations provided for in sub-paragraph 2(b) or (c) above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

4. Any Party which has excluded certain categories of automated personal data files by a declaration provided for in subparagraph 2(a) above may not claim the application of this Convention to such categories by a Party which has not excluded them.

5. Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraph 2(b) and (c) above may not claim the application of this Convention on these points with respect to a Party which has made such extensions.

6. The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the Convention with regard to the State which has made them at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been formulated at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

Chapter II—Basic Principles For Data Protection

Article 4—Duties of the Parties

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2. These measures shall be taken at the latest at the time of entry into force of this Convention in respect of that Party.

Article 5—Quality of data

Personal data undergoing automatic processing shall be:

a) obtained and processed fairly and lawfully;

b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purpose for which they are stored;

d) accurate and, where necessary, kept up-to-date;

e) preserved in a form which permits identification of the data subjects

for no longer than is required for the purpose for which those data are stored.

Article 6—Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7—Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.

Article 8—Additional safeguards for the data subject

Any person shall be enabled:

a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;

d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs (b) and (c) of this article is not complied with.

Article 9—Exceptions and restrictions

1. No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed where such derogation provided for by the law of the Party constitutes a necessary measure in a democratic society in the interests of:

a) protecting state security, public safety, the monetary interests of the State or the suppression of criminal offences;

b) protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs (b), (c) and (d) may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10—Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11—Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention.

Chapter III—Transborder Data Flows

Article 12—Transborder flows of personal data and domestic law

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party.

3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:

a) insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;

b) when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

Chapter IV—Mutual Assistance

Article 13—Cooperation between Parties

1. The Parties agree to render each other mutual assistance in order to implement this Convention.

2. For that purpose:

a) each Party shall designate one or more authorities the name and

address of each of which it shall communicate to the Secretary General of the Council of Europe;

b) each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.

3. An authority designated by a Party shall at the request of an authority designated by another Party:

a) furnish information on its law and administrative practice in the field of data protection;

b) for the sole purpose of protection of privacy, take all appropriate measures, in conformity with its domestic law, for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14—Assistance to data subjects resident abroad

1. Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this Convention.

2. When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

3. The request for assistance shall contain all the necessary particulars, relating inter alia to:

a) the name, address and any other relevant particulars identifying the person making the request;

b) the automated personal data file to which the request pertains, or its controller;

c) the nature of the request.

Article 15—Safeguards concerning assistance rendered by designated authorities

1. An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.

2. Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate restrictions of secrecy or confidentiality with regard to that information.

3. In no case may a designated authority be allowed to make a request for assistance on behalf of a data subject resident abroad, as referred to in Article 14, paragraph 2 of its own accord and without the express consent of the person concerned.

Article 16—Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this Convention may not refuse to comply with it unless:

a) the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;

b) the request does not comply with the provisions of this Convention;

c) compliance with the request would be incompatible with the sovereignty, security or public policy (ordre public) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

Article 17—Costs and procedures of assistance

1. Mutual assistance which the Parties render each other under Article 13, and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.

2. The data subject may be charged no costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.

3. Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

Chapter V—Consultative Committee

Article 18—Composition of the Committee

1. A Consultative Committee shall be set up after the entry into force of this Convention.

2. Each Party shall appoint a representative to the Committee and a deputy representative. Any Member State of the Council of Europe which is not a Party to the Convention shall have the right to be represented on the Committee by an observer.

3. The Consultative Committee may, by unanimous decision, invite any non-Member State of the Council of Europe which is not a Party to the Convention to be represented by an observer at any of its meetings.

Article 19—Functions of the Committee

The Consultative Committee:

a) may make proposals with a view to facilitating or improving the application of the Convention;

b) may make proposals for amendment of this Convention in conformity with Article 21;

c) shall formulate its opinion on any proposal for amendment of this Convention which is referred to it in conformity with Article 21, paragraph 3;

d) may, at the request of a Party, express an opinion on any question concerning the application of this Convention.

Article 20—Procedure

1. The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this Convention. It shall subsequently meet at least once every two years and in any case when one third of the representatives of the Parties request its convocation.

2. A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.

3. After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the Convention.

4. Subject to the provisions of this Convention, the Consultative Committee shall draw up its own Rules of Procedure.

Chapter VI—Amendments

Article 21—Amendments

1. Amendments to this Convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.

2. Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the Member States of the Council of Europe and to every non-Member State which has acceded to or has been invited to accede to this Convention in accordance with the provisions of Article 23.

3. Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee which shall submit to the Committee of Ministers its opinion on that proposed amendment.

4. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.

5. The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.

6. Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Chapter VII—Final Clauses

Article 22—Entry into force

1. This Convention shall be open for signature by the Member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five Member States of the Council of Europe have expressed their consent to be bound by the Convention in accordance with the provisions of the preceding paragraph.

3. In respect of any Member State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of the instrument of ratification, acceptance or approval.

Article 23—Accession by non-Member States

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided by Article 20(d) of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee.

2. In respect of any acceding State, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification with the Secretary General of the Council of Europe.

Article 24—Territorial clause

1. Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of

the month following the expiration of a period of three months after the date of receipt by the Secretary General of such declaration.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25—Reservations

No reservation may be made in respect of the provisions of this Convention.

Article 26—Denunciation

1. Any Party may at any time denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27—Notifications

The Secretary General of the Council of Europe shall notify the Member States of the Council and any State which has acceded to this Convention of:

a) any signature;

b) the deposit of any instrument of ratification, acceptance, approval or accession;

c) any date of entry into force of this Convention in accordance with Articles 22, 23 and 24;

d) any other act, notification or communication relating to this Convention.

RECOMMENDATION OF THE COUNCIL

Concerning Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data

(23rd September, 1980)

THE COUNCIL,

Having regard to articles 1*(c)*, 3*(a)* and 5*(b)* of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

RECOGNISING:

that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;
that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;
that transborder flows of personal data contribute to economic and social development;
that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;

2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;

4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

ANNEX TO THE RECOMMENDATION OF THE COUNCIL OF 23RD SEPTEMBER 1980

Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data

Part One: General

Definitions

1. For the purposes of these Guidelines:

a) "data controller" means a party who, according to domestic law, is

competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

b) "personal data" means any information relating to an identified or identifiable individual (data subject);

c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

a) the application, to different catagories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

a) as few as possible, and

b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

Part Two: Basic Principles Of National Application

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or
b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identify and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him
   i) within a reasonable time;
   ii) at a charge, if any, that is not excessive;
   iii) in a reasonable manner; and
   iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs *(a)* and *(b)* is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Part Three: Basic Principles Of International Application: Free Flow And Legitimate Restrictions

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

Part Four: National Implementation

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

a) adopt appropriate domestic legislation;
b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
c) provide for reasonable means for individuals to exercise their rights;

d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
e) ensure that there is no unfair discrimination against data subjects.

Part Five: International Co-Operation

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

i) information exchange related to these Guidelines, and
ii) mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

NOTES

[1] For a discussion of the difficulty in defining "data processing" see *infra* text accompanying note 29.

[2] Hessisches Datenschutzgesetz, 1970 Gesetz- und Verordnungsblatt für das Land Hessen 625; *see also* F. HONDIUS, EMERGING DATA PROTECTION IN EUROPE 35-36 (1975)(summary of Hessian law).

[3] Datalagen, 1973 SFS 289 (amended 1977)(Swed.), *reprinted in* 2 TRANSBORDER DATA FLOWS: CONCERNS IN PRIVACY PROTECTION AND FREE FLOW OF INFORMATION (R. Turn ed. 1979)[hereinafter cited as TRANSBORDER DATA FLOWS].

[4] *See, e.g.*, Loi relative a l'informatique, aux fishiers et aux libertés, 1978 Journal Officiel de la République Française 227F (Fr.); *see also* 2 TRANSBORDER DATA FLOWS (reprints laws of Austria, Denmark, the Federal Republic of Germany and Norway).

[5] Privacy Act of 1974, 5 U.S.C. § 552(a)(1976)(U.S.); Human Rights Act, ch. 33, 1976-1977 Can. Stat. 887 (Can.), *both reprinted in* 2 TRANSBORDER DATA FLOWS, *supra* note 3; *see also* TRANSNAT'L DATA REP., Jan. 1983, at 12 (by 1984 data protection legislation will be enacted in the following countries: Australia, Belgium, Finland, Japan, the Netherlands, Portugal, Spain, Switzerland and the United Kingdom).

[6] *See* Statute of the Council of Europe, May 5, 1949, Europ. T.S. No. 1, *reprinted in* A. PEASLEE, 1 INTERNATIONAL GOVERNMENTAL ORGANIZATIONS: CONSTITUTIONAL DOCUMENTS 341 (3d ed. 1974) [hereinafter cited as PEASLEE]. The goal of the Council is to achieve "a greater unity between its members for the purpose of safeguarding and realizing the ideals and principles which are their common heritage and facilitating their economic and social progress." *Id.* at art. 1.

Membership in the Council is limited to states which "accept the principles of the rule of law and of the enjoyment by all persons within their jurisdiction of human rights and fundamental freedoms." *Id.* at art. 3.

7 Founded in 1968 under the formal title: Committee of Experts on the harmonization of the means of programming legal data into computers.

8 *See* Convention on the Organization for Economic Cooperation and Development, Dec. 14, 1960, *reprinted in* 2 PEASLEE, *supra* note 6, at 1154. The OECD was established to succeed the Organization for European Economic Cooperation. The OECD's objectives are to promote economic and social welfare within OECD member states by assisting in the formulation of national legislation. It is also active in harmonizing member state efforts to aid less developed countries. *Id.* at art. 1.

9 Council of Eur. Res. 73(22)(1973), *reprinted in* 2 TRANSBORDER DATA FLOWS, *supra* note 3.

10 Council of Eur. Res. 74(29) (1974), *reprinted in* 2 TRANSBORDER DATA FLOWS, *supra* note 3.

11 *Opened for signature* Jan. 28, 1980, Europ. T.S. 108 [hereinafter cited as Convention]. The Convention is reprinted at the end of the article.

12 *See* Working Party on Information, Computer and Communications Policy, Draft Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. No. DSTI/ICCP/79.40 (1977), *reprinted in* 2 TRANSBORDER DATA FLOWS.

13 *See* OECD, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1981) [hereinafter cited as GUIDELINES]. The GUIDELINES are reprinted at the end of the article. Australia, Canada, Ireland, Turkey and the United Kingdom abstained from the Recommendation of the Council of OECD promulgating the GUIDELINES. *Id.* at preface.

14 According to some observers, the different focuses of these two organizations, as reflected in their preambles, is explained by their respective "missions." *See* Patrick, *Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and the OECD Guidelines,* 21 JURIMETRICS 405, 409 (1981).

15 This indicates the close ties between the two organizations, both between the secretariats and as a result of the number of overlapping delegates.

16 The Council of Europe's goal, *inter alia,* is to "extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing." Convention, *supra* note 11, at preamble. This concentration on the human rights aspect is immediately followed by an affirmation of the Council's "commitment to freedom of information regardless of frontiers." *Id.*

The OECD directly addresses the conflict: "[member states] have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information." GUIDELINES, *supra* note 13, at 7.

Thus, both organizations recognize the conflict, albeit for different reasons. *See* Patrick, *supra* note 14, at 409.

17 The wording of the definition reveals that the terms "data" and "information" are used interchangeably. *Compare* J. BING, TRANSNATIONAL DATA FLOWS AND SCANDINAVIAN DATA PROTECTION LEGISLATION 68 n.2 (1980)(in technical parlance the two terms have distinct meanings).

18 *See generally* J. BING, PERSONAL DATA SYSTEMS–A COMPARATIVE PERSPECTIVE ON A BASIC CONCEPT IN PRIVACY LEGISLATION (1979).

19 GUIDELINES, *supra* note 13, at 25 (their Explanatory Memorandum states that "the Guidelines deal with the building up and use of aggregates of data which are organized for retrieval, decision-making, research, surveys and similar purposes."). Future references to the GUIDELINES refer to the Explanatory Memorandum [hereinafter cited as Explanatory Memorandum].

20 Seipel, *Transborder Flows of Personal Data,* TRANSNAT'L DATA REP., Jan. 1981, at 32.

21 *See* Expert Group on Transborder Data Barriers and the Protection of Privacy, Statement by U.S. Delegation, OECD Doc. No. DSTI/ICCP/78.45, at § 21(a)(1977).

22 *See supra* text accompanying note 19.

23 *See* 2 TRANSBORDER DATA FLOWS, *supra* note 3, for the English translations of these laws.

24 Explanatory Memorandum, supra note 19, at 27 ("The Guidelines should not be applied in a mechanistic way . . .").

25 *Id.*

26 Australia, Canada, New Zealand, the United Kingdom and the United States.

27 In its 1984 work program proposals, the OECD Committee on Information, Computer and Communications Policy has suggested that the study of liability in international data networks, the study of insurance in international data services and the feasability of an international scheme for authentification of computer transactions should be given priority among the legal issues in transborder data flows. *See* OECD Doc. No. DSTI/ICCP/83.6, at 10 ( ).

28 *See Seipel, supra* note 20, at 36.

29 *See generally* R. BLEKELI, FRAMEWORK FOR THE ANALYSIS OF PRIVACY AND INFORMATION SYSTEMS (1979).

30 *Id.* at 27.

31 For a discussion of the principle of adequacy in national legislation see Bing, *A Comparative Outline of Privacy Legislation*, 1978 COMP. L.Y.B. 170, 170-173.

32 An example illustrates the potential for abuse in data collection if the collector does not have limits placed on the purpose for which data may be collected: a Norwegian bank collected data on individuals who were very active in extremist left-wing groups and circulated this information to its depositors. Under the Convention and GUIDELINES approach, so long as the purpose was stated before collection, it would not be unlawful. Norwegian law, on the other hand, would probably prohibit the bank's conduct because the purpose for which the data was collected was not related to banking. *See* 2 TRANSBORDER DATA FLOWS, *supra* note 3, for the text of the Norwegian law; *see also* HONDIUS, *supra* note 2, at 42-44.

33 *See* 2 TRANSBORDER DATA FLOWS, *supra* note 3. In particular the laws of Denmark (pt. 3, § 9(2)), France (ch. 4, § 31), Norway (¶¶6 & 9) and Sweden (§ 4) limit the collection of sensitive data. *See also* Bing, *supra* note 31, at 174-75.

34 *Cf.* BING, *supra* note 17 (Convention's list of sensitive data corresponds to most European national laws).

35 Explanatory Memorandum, *supra* note 19, at 28.

36 The Explanatory Memorandum notes that personal data is "completely excluded from the application of the Guidelines." *Supra* note 18, at 27. This implies that national legislation in this area is contemplated, subject to the proviso that it is not "regarded as a vehicle for demolishing the standards set up by the Guidelines." *Id.*

37 The Explanatory Memorandum states that "data which have been collected for purposes of administrative decision-making may be made available for research, statistics and social planning." *Id.* at 30.

38 *Id.*

39 *See* 2 TRANSBORDER DATA FLOWS, *supra* note 3. In particular the laws of Denmark (pt. 2, § 6(4)), Germany (§ 6), Sweden (§ 6) and the United States (§ 552(a)) make reference to data security. *See also* Bing, *supra* note 31, at 175.

40 *See, e.g.*, Loi relative a l'informatique, ch. III, art. 22, 1978 J.O. 229 (Fr.) (public notice); Privacy Act of 1974, 5 U.S.C. § 3(f)(5)(1976)(*id.*); Datalagen, § 10 (Swed.) (access to records), *reprinted in* 2 TRANSBORDER DATA FLOWS, *supra* note 3; *see also* Bing, *supra* note 31, at 176.

41 There is a small difference in wording between the Convention, which defines address as "habitual residence or principle place of business" (art. 8(2)), and the GUIDELINES, which refer to "usual residence" (¶ 12). This is probably a negligible distinction, although the

GUIDELINES approach is less precise than the term "habitual residence," which has independent meaning in international law.

[42] *See supra* text accompanying note 39.

[43] *See, e.g.*, the Norwegian (¶ 7) and Danish (§§ 13-15) laws, *reprinted in* 2 TRANSBORDER DATA FLOWS, *supra* note 3.

[44] Explanatory Memorandum, *supra* note 19, at 34.

[45] *Compare id. with* Convention, *supra* note 11 (explicit denial of mandate in Explanatory Memorandum of GUIDELINES vs. silence in Convention).

[46] *See* Bing, Forsberg & Nygard, *Legal Issues Related to Transborder Data Flows*, in POLICY IMPLICATIONS OF DATA NETWORK DEVELOPMENTS IN THE OECD AREA 62 (OECD 1980).

[47] *Cf.* S. SIMITIS, U. DAMMAN, O. MALTMANN & H. REH, KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ: NOMOS, BADE-BADEN 550 (1976)(notes that German act has been interpreted so that the relative level of protection is the main reference for regulating transnational data flows).

[48] *See* LINDOP COMMITTEE, REPORT OF THE COMMITTEE ON DATA PROTECTION 246 (1978)(HSMO).

[49] *See generally* Bing *et.al, supra* note 46.

[50] *See supra* text accompanying note 11.

[51] *See* Explanatory Memorandum, *supra* note 19, at 35.