The John Marshall Journal of Information Technology & Privacy Law

Volume 11
Issue 3 *Computer/Law Journal - Fall 1992*

Article 2

Fall 1992

An EEC Policy for Data Protection, 11 Computer L.J. 399 (1992)

Peter Blume

AN EEC POLICY FOR DATA PROTECTION

by PETER BLUME*

"If we are not to be lurched headlong by the chariot of technology but are to preserve our basic values—and protect them by law—we must do better than we have in the recent past. The hare of technology rushes ahead. The tortoise of legal protection dawdles aimless, lost, bewildered, far behind."[1]

I. THE REASONS FOR DATA PROTECTION

The emergence of computer technology and its dominant position in most developed countries has, among other things, led to an increased need to consider the legal protection of privacy with respect to information. It has been a long standing assumption that the use of computer systems for handling personal information implies new risks for invasions of privacy and, as we live at a time in history when privacy is highly regarded,[2] legal regulations that implement restraints on the use of computer technology become necessary. The approach to the privacy problem is not the same in all countries but has been most thoroughly developed in Europe, where several countries have enacted special data protection laws and the European Council has issued a Data Convention.

The main part of this article will directly or indirectly consider the problems caused by the lack of a global consensus on the appropriate level of data protection now being emphasized by the initiative taken by the EEC Commission, which will be described in more detail below. Before doing this, the article will briefly consider why the computer in particular raises privacy questions and how these questions are tackled

* Peter Blume is an associate professor, Doctor of law, University of Copenhagen, Copenhagen, Denmark.

1. Kirby, *Computer Law & Security Rep.*, Vol. 6, No. 1 at 29 (1990).

2. Whether privacy is regarded as necessary or whether citizens accept mutual knowledge about each other depends on the general ideologies in society. Privacy is no necessity and what kind of data protection is deemed appropriate will differ from society to society. *See, e.g.*, C.C. GOTLIEB & A. BORODIN, SOCIAL ISSUES IN COMPUTING 71 (New York 1974).

in some countries and in international regulations. The perspective will by mainly European, but as is elaborated in the final section, the purpose of this article is to emphasize the growing need for a transatlantic discussion due to the emergence of a global information market.

Compared to the old methods of storing, retrieving and using information, computer technology has several advantages that makes it natural to use this technology. It is possible to keep much more information in one system. The storage capacity of databanks technically has no real limits, which means that the well-known tendency of mainly public authorities to collect information is sustained. It becomes possible to keep extensive amounts of personal data in public files, which in itself emphasizes the latent conflict between individual and state. It should be added, however, that a tendency to store excessive amounts of information also occurs in the private sector.

Storage of information, however, is not the major consequence of the computer. Much more disturbing from the perspective of privacy are the methods made available by computer technology for handling the stored information and for communicating it. Storage of vast amounts of information makes little sense if it is not practical to identify and use the data. The computer, to a large extent, solves these problems. Specific data can be located and retrieved extremely quickly and data can just as quickly be combined with other relevant information, e.g., all data relating to a certain individual. Use of personal data can be very sophisticated. It is important to note in particular that data from different files can easily be combined and matched, thereby leading to the creation of a profile of an individual citizen. The ease of retrieval furthermore implies that data can be communicated without difficulty to third parties and distributed in wider and wider circles.

As is well-known, developments involving computer technology have been rapid, both with respect to the technology, such as personal computers and integrated/open networks, as well as the qualitative use of computers, such as the development of decision support systems and expert systems.[3] At the same time information has become an increasingly important commodity[4] both in the private and public sectors, leading to the general desirability of information flow.

---

3. Still new problems face data protection, see COUNCIL OF EUROPE, NEW TECHNOLOGIES: A CHALLENGE TO PRIVACY PROTECTION? (Strassbourg 1989).

4. Information is a somewhat special commodity as its value is relative. For some a piece of information has high value, for others no value at all. It is also a characteristic that once information has been communicated it cannot be taken back. It falls outside this article to discuss in detail the special nature of information. *See* H. COLLIER, INFORMATION FLOW ACROSS FRONTIERS 1 (Oxford 1988).

In this article *information* and *data* are used as synonyms.

It is with this background that the legal protection of individual citizens is necessary. Although use of manually processed data can also endanger privacy, this protection is particularly needed for computerized data. This is especially true since privacy is one of the fundamental human rights, as stated in Article 8 in the European Convention of Human Rights. The human rights dimension is discussed further below. It should be noted here, however, that it is also a human right to send and receive information (e.g., the European Convention Article 10) and that this right in some respects must be balanced against the right to privacy.

The human rights aspect emphasizes the importance of data protection and makes it clear that this area must be of primary interest to computer lawyers and is a field of growing importance due to the amount of computer-based information that is of a personal nature. This is also the reason why the issue of data protection has expanded from being a primarily European matter to an issue of global importance, as illustrated by the promulgation of a data protection act for the private sector in Japan in 1988 that came into force in 1989.

II. NATIONAL REGULATION

The first data protection statute was enacted in the West German state of Hessen in 1970 and the first national statute was enacted in Sweden in 1973. In 1978 three other countries, Denmark, Norway and France, enacted statutes. Today such laws are found in many European countries while bills are being considered in several others.[5] The European data protection acts differ in many respects, which is one of the reasons for the EEC initiative discussed below.

In this section the national regulations on data protection will be illustrated by reference to the Scandinavian model, in particular the Danish rules which are a typical example of first generation legislation. Denmark, as a member of the EEC, provides a link between the Community and the Nordic countries and for this reason is a good example to use.

In Denmark there are two data protection acts concerning the private and the public sectors. This is due to the fact that legitimate reasons for registration and recording can be different in the two sectors.[6] Although there are many differences between the two acts some of the main features are identical.

---

5. The first East European country likely to enact legislation will be Hungary where the cabinet agreed upon a bill in January 1989.

6. The acts from 1978 with amendments in 1987 are described in detail in P. BLUME, PERSONREGISTRERING (Copenhagen 1987) (in Danish). The amendment act is described by Peter Blume in INT'L COMPUTER L. ADVISER, Vol. 3, No. 2, at 16-19.

Personal data can only be recorded if authorized by the Act. As a starting point it is the character of the data that determines whether a certain piece of information can be recorded. A distinction is made between ordinary and sensitive information, e.g., that information concerning political beliefs and sexual attitudes. The conditions for registration of sensitive information are severe. Most private firms will not be allowed to record such information and it is, for example, absolutely forbidden for credit rating agencies. According to the same principles, distribution of recorded information depends on the nature of the data and, in the public sector, also on whether the receiver is another authority or a private firm.

Data controllers in most cases are obliged to give citizens access to their files so they can check the stored information. The right of access is considered a very important right, but both in Denmark and in other countries it is seldom used. The data controller must ensure high data quality in his files and is only allowed to store actual information. Data security is also the responsibility of the data controller.

The rules are controlled by the Data Inspectorate, which is a department under the Ministry of Justice, and in the private sector several rules are backed by criminal sanctions.

All in all the two Danish acts aim at a high level of protection and, as computer technology has developed, the constraints on business and on public authorities have been felt much more than before. However, it is still the Danish position that such rules are necessary.

Seen from an international perspective, it is to some extent the mode of protection rather than the individual rules which is of interest. It is characteristic of Scandinavian data protection laws that their aim is to state exact rules. In many respects, particularly in the private sector, the statutory rules stand alone and are only supplemented by the practice of the Inspectorate. This is not a generally accepted model of regulation. In other countries, such as England (Data Protection Act 1984) and Holland (wet persoonregistraties 28/12, 1988), the rules are based upon self-regulation and outline a set of general principles which the data controllers are expected to follow.[7] This can lead to another form of conflict resolution which is not as liberal as the statutory form would indicate. It is, for example, interesting to note that while in Denmark there has been only one court case for a violation of the data protection

7. On the principles in the English act, see R. WACKS, PERSONAL INFORMATION 210-21 (Oxford 1989).

acts, in England there are many such cases annually.[8] The English form of regulation is not as liberal in practice as the Danish.

Even when such circumstances are taken into account the various ways in which data protection acts are drafted create a major problem for a harmonized international regulation, since it is very difficult to estimate whether the different rules lead to the same results, i.e., whether the practice is identical. This is particularly true when the question of transborder data flow is considered.

As can be seen, data protection is regulated differently in the countries which have taken the question seriously. It is also clear that much of the legislation is still quite experimental and it is uncertain which method is best to protect citizens against some of the dangers that data technology can cause.

III. INTERNATIONAL REGULATION

At the beginning of the 1980s two sets of international rules concerning data protection were issued. It was recognized by then that data technology in particular could lead to new kinds of invasion of privacy and that this should not be regarded as mainly a national problem. The world was becoming smaller and the economic and social relationships of many countries were much closer than had previously been the case. The global market was beginning to emerge. This, among other things, led to an increased need for distribution of information across borders. As much of this information is of a personal nature, and as the needs of the market should not undermine the legal protection of citizens, it became increasingly necessary to regulate the use of personal data similarly in the different countries.

Accordingly, the existing international rules have two main purposes—first, to ensure a certain level of protection and second, to make transborder data flow possible in an acceptable way.

The general problem of these rules, and the forthcoming EEC rules as well, is the difficulty of assuring that national rules are equivalent. An important policy problem is to reach an understanding of what *equivalence* means. The problem is whether it is sufficient that the same principles are followed in the different countries, or if the principles should also be implemented in the same way so that a truly uniform regulation occurs. In connection with the categorization of different kinds of data, the problem is whether the same data should be considered sensitive everywhere or whether each country should be allowed to place varied or additional data types on the list. It seems clear

8. The Danish case concerned registration of sensitive information by the Scientology Church, which lost the case. Illustrative for English practice is the statistics given in the *Data Protection Registrar, Annual Report 1989*, at 19-20.

that if the former situation is permitted, there will be instances where data cannot flow freely if equivalence means similar rules. A totally open market with no borders seem to presuppose that a harmonized regulation is achieved if the legal protection of citizens is to be taken seriously. On the other hand there are different legal and political traditions which can make it almost impossible to achieve this goal unless a binding international cooperation exists.

Accordingly, the problem of equivalence makes it necessary to consider how dangerous transborder data flow can be and how these dangers should be evaluated when the benefits of information exchange for trade and citizens are considered. With this background it would seem appropriate to make the character of the different data types the starting point and to limit the strict notion of equivalence to sensitive data and records. This possibility will be discussed in more detail below.

A. OECD

On September 23, 1980, the Committee of Ministers of the OECD issued *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.[9] The *Guidelines* have been endorsed by all twenty-four member states and are the international rules accepted by most countries today. The *Guidelines* do not constitute a legally binding instrument, but the member countries have declared their intention to follow the rules. The practical importance of the *Guidelines* varies according to the domestic legislation of the individual country and whether it has submitted to other international obligations.

The impact of the *Guidelines* is greatest in countries which have a weak or incomplete data protection level. This is demonstrated in two ways. First, there are several companies in the United States and Canada, for example, which have endorsed the principles as their ethical principles as part of their company policy.[10] Second, data commissioners, as in Australia, have encouraged companies to respect the *Guidelines*.[11] It can be assumed that the principles laid down in these fairly old *Guidelines* are recognized in most developed countries.

The *Guidelines* are divided into two main parts. In the first part (Articles 7-14) the basic principles for data protection are outlined. These principles concern collection limitation, data quality, purpose

9. On the preparation of the *Guidelines* see R. WEITH, MULTINATIONAL COMPUTER NETS 16-17 (Toronto 1981). *See also* J. DE HOUWER, K. VAN BRABANT, THE TRANSBORDER FLOW OF PERSONAL DATA 19-25 (Vriije Universiteit, Bruxelles 1989).

10. The companies have expressed a wish to have the practical consequences of endorsement clarified. *See* L. Hummer, *in* TRANSBORDER DATA FLOWS: PROCEEDINGS OF AN OECD CONFERENCE 45 (Amsterdam 1985).

11. *See* Kirby, *The Computer Law and Security Report*, Vol. 6, No. 1, at 27 (1990).

specification, use limitation, security safeguards, openness, individual participation and accountability. Rules of this kind should be implemented in national legislation. It should be noted that these principles are not formulated very precisely, and accordingly, there are many ways in which they can be fulfilled. There is no guarantee against major differences between legislation in countries which respect the principles. As indicated above, this is an important observation when international regulations as a whole are evaluated.

In the second part the principle of free flow of information across borders is stated (Articles 15-18). Countries which have fulfilled the basic principles in their national legislation must allow data to flow freely, i.e., without any need for prior permission, except in two situations. The first is the most interesting. If the legislation of one state contains rules that are not found in the laws of the other state, data export can be restricted. This is the principle of *equivalence*. As the *Guidelines* are very broadly drafted this situation will often occur. Second, data export cannot take place if the receiving state only functions as a transit country for a state which has not implemented the *Guidelines*. The purpose of this rule is to prevent covert data havens.

All in all the *OECD Guidelines* contain the most important data protection principles and also clearly state the principle that data should be transferable across borders. As there are many possibilities of derogation and as the rules are not legally binding, the *Guidelines* are not sufficient to ensure the functioning of the global information market.

B. THE EUROPEAN COUNCIL

To a large degree the comments on the OECD rules apply to the Convention of the Council of Europe—*For the Protection of Individuals with Regard to Automatic Processing of Personal Data* (No. 108/1981)—which came into force in 1985. This is, however, a real treaty binding on the countries which have ratified it. Today ten countries, including seven EEC countries, have ratified the convention and all twenty-three member countries have signed it, thereby expressing an intention to ratify it. The convention is, accordingly, the most important instrument in the data protection area today.

In many ways it is natural that the European Council regulate data protection, since the Council is in charge of the European Convention on Human Rights and, as mentioned above, two human rights play an important role in this area. The first is the right to privacy outlined in the Convention's Article 8. It is not strange that in some countries, including the United States, the phrase "privacy" is preferred over "data protection."

It is necessary to add some remarks concerning the human right to privacy. Traditionally, human rights have been viewed as legal rules concerning the relationship between the state and its citizens. From this point of view privacy only makes it necessary to have data protection rules in the public sector. This is, however, an inadequate approach where a fundamental conflict between the individual and private enterprise can also exist. The privacy issue is relevant in the private sector as well and it is not appropriate to let this sector go unregulated. It is natural, therefore, that the Data Convention covers both the public and private sectors.

The other human right is the freedom of expression in Article 10, including a right "to receive and impart information . . . regardless of frontiers." It is easy to see that these two rights can contradict one another in some situations and that it is necessary to balance them. There are no clear rules for how such a balance can be achieved and it is not possible to assume that one of the rights ought to be given priority over the other. The Data Convention can be seen as an attempt to balance these rights, in particular with regard to transborder data flow.

The Convention is structured in the same way as the *OECD Guidelines*, which is not strange as it was drafted at the same time (1980). In Articles 5-10 the basic data protection principles are outlined. The principles are fairly broadly formulated and it is particularly interesting that there are several possibilities for derogation. With the exception of the principle of sufficient data security, the principles can be derogated according to Article 9 for specific reasons, e.g., state security. Article 11 emphasizes that national rules can give citizens a wider measure of protection than follows from the principles. These possibilities are important when assessing transborder data flow, which is regulated in Article 12 in the same way as in the *OECD Guidelines*. There will be many situations where the principle of equivalence is not fulfilled. This is one of the reasons for the EEC initiatives discussed below.

The Convention recognizes that modern technology constantly creates new challenges to data protection and that these challenges can vary within different sectors of society. The problems are being considered by an expert committee which has drafted several recommendations that have been approved by representatives of the member countries.[12] Although these recommendations are not legally binding, their approval signifies an intention to respect them. The recommendations, however, are drafted fairly broadly and, in the same way as the Convention itself, they do not guarantee that there will be an equivalent level of protection in the different countries. The sectorial

12. Today there are six recommendations, including such subjects as automated medical data banks (R(81)1) and personal data used for employment purposes (R(89)2).

approach taken by the European Council is interesting as it shows that the general provisions on data protection must be supplemented with special rules. This approach will also be taken by the EEC after its general directive has been implemented.

Although there are deficiencies in the European Convention, the Convention is the most important international instrument today. This will change, however, when the EEC initiatives have been implemented.

IV. THE EUROPEAN COMMUNITY

For many years the European Parliament and the EEC Commission have taken an interest in data protection and have tried to encourage member countries to enact rules and to ratify the European Convention.[13] As of January 1991, only seven countries[14] had ratified the Convention, and among these, one country, Spain, had no data protection legislation as its ratification was founded upon provisions in the Spanish constitution. One of the five non-ratifying countries, Holland, has a data protection act and will probably soon ratify. The other four, Belgium, Italy, Portugal and Greece, have no legislation. Accordingly, it is fair to state that the situation generally speaking is unsatisfactory within the Community and that the legal protection of the European citizen is not at an adequate level.

There are several reasons for the Commission to rectify this situation. The most important is the emergence of the single market, which should be completed by January 1, 1993. This market will have immense importance from a global perspective, since it is founded upon the removal of borders with the implication that goods and services will flow freely within the market. As is well-known, information is extremely important for both private enterprise and public authorities, particularly when borders are removed. It is accordingly necessary that information flow freely within the market. For the private sector information flow will increase the global competitiveness of the market, and in the public sector information flow seems to be a condition for the maintenance of law and order when national borders are broken down.

While the emergence of the single market can explain why the initiative is being undertaken now, there are also other general considerations which makes an EEC regulation appropriate. The Community is attaching increased importance on the protection of human rights and

13. Resolutions to this effect from the European Parliament are published in the *Official Journal of the European Communities*, section C, 1976 (100/27), 1979 (140/34) and 1982 (87/39).

14. These countries are Denmark, England, France, Germany, Ireland, Luxembourg and Spain.

the legal protection of the European citizen. The proposed rules can be viewed as part of the EEC's so-called *social dimension*, emphasizing that the community is more than an economic cooperation. In general the aim of the rules is a high level of protection. This fact is important since it leads to certain rules which, when seen from a pure economic point of view, are unfortunate.

In July 1990 the Commission finalized a packet of proposals (COM(90)314 FINAL) which were presented to the different community organs, where they are now being discussed. The primary proposal is a Council draft directive "concerning the protection of individuals in relation to the processing of personal data." This general directive, which has authority in Articles 100A and 113 of the Treaty of Rome, is discussed in detail below. (A copy of the proposed data protection directive is reprinted as an appendix to this article.) Attached to the directive is a proposal that the Council recommends to the member states that public records not covered by EEC law in national legislation be governed by the same rules. The Council should also decide that the Community as such adheres to the European Council Data Convention, which will provide a framework for negotiations with third countries with respect to data exports.

The Commission will issue a self-binding declaration according to which the directive will also apply to files held by EEC institutions. Furthermore, it is proposed to issue a special directive "concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public mobile networks." Finally, the Council should instigate a two year action plan with the aim of establishing a common regulation of information security. All in all a quite impressive series of proposals. The following discussion will centre on the general directive which is the most important.

A. The General Scope

The proposed general directive covers all electronic files and structured manual files. Although the need for data protection in particular has been linked to the computerization of data and although, as mentioned above, there are special risks attached to electronic files, it is clear that data in other forms can also be misused for invasions of privacy. It is also easier for data users to organize their activities if the same rules can be applied in all situations. Accordingly, the draft directive only contains a few special rules for computerized data.

The directive covers the public sector with the exceptions mentioned above and covers the private sector except for two kinds of files mentioned in Article 3. First, files held by "an individual solely for pri-

vate and personal purposes" are not covered. This exception is due to the fact that these files fall within the protection of privacy in the Convention of Human Rights. Furthermore, of course, it is quite impossible to enforce rules concerning such files.[15] This exception does not seem to raise any difficulties.

The second exception is for files of "non-profit making bodies" when the file only relates to members who have consented to being included in the file and if the filed information is not communicated to third parties. This exception also seems obvious and in accordance with the special status many constitutions give to such associations.

Since the directive, which is documented below, is so far-reaching, it is very important which form of regulation is applied. The rules can generally be characterized as fairly bureaucratic and at the same time very strict. They aim at a very high level of protection which can easily become impractical. Although the draft directive contains many good rules, the general feeling is that the privacy issue is overstated with the risk that it will not be taken sufficiently seriously in practice. As data protection rules are very difficult to enforce, they are dependent on the acceptance and understanding of data users; very bureaucratic rules therefore can be counterproductive. Consequently, it seems doubtful whether all the proposed rules are workable and whether the good intentions can be fulfilled. After these general comments it is time to take a look at the different rules and in this connection to address the criticism that has been raised to them.

B. FREE DATA FLOW

The general purpose of the directive is made clear in Article 1, in subsection 2, where it is stated that member states cannot restrict or prohibit the free flow of personal data within the Community for reasons of data protection within the rules of the directive. This means that even though the directive offers some possibilities for individual states to enact special rules, these rules cannot impeded data exports to other member states. This is important since the directive thereby circumvents the problems of the European Convention and makes it clear that it is the general rules of the directive which provide the level of protection. As a consequence the importance of the individual rules in the directive increases.

When data protection rules cover many individual states the question of jurisdiction becomes very important. As a practical condition for the possibilities of citizens to enforce their rights, it is necessary that it be easy to define the relevant data protection authority and that there

15. However, in Denmark such electronic files are illegal today for the private sector to section 1 of the Data Protection Act.

be one clear jurisdiction. It is the intention of Article 4 to solve this problem. It states that the physical location of a file determines which country's rules are applicable. If a file located in a country outside the Community that does not provide an adequate level of protection is searched, the member country in which the person is living has jurisdiction. This is generally a clear rule which prevents the unfortunate situation where conflicting laws are applicable. However, in practice it can provide problems for citizens when data is transmitted directly to a file in another country whose legislation accordingly applies.[16] It must be expected that the local data protection authority will assist its citizens in such situations. Even though concerns about this rule have been expressed, it is preferable to the silence of the European Convention where there is no solution to the question of jurisdiction.[17]

C. REGISTRATION AND COMMUNICATION

Parallel to the aforementioned Danish regulation, the rules concerning when personal information can be recorded and distributed are different for the public and private sector. This is fortunate as the legitimate reasons for registration are different in the two sectors.

1. *Public Sector*

The rules concerning the public sector are found in Articles 5-7 and 17. As for recording, the general rule is that a file can be created when it is "necessary for the performance of the tasks of the public authority in control of the file" (5, litra a). This is not a very precise rule, but emphasis should be placed upon the word "necessary" and in practice the lawfulness of a registration will depend upon a comparison between the nature of the information and the tasks of the authority. This often difficult evaluation can be aided by the notification procedure described below. It is not possible in a general rule to outline all the reasons that can make filing legitimate.

It is a common situation that after information has been filed for a certain purpose, it can be used for other purposes. A general data protection principle is that information should only be used for the reasons which made its recording legitimate.[18] As this can be quite impractical it is necessary to state when this principle can be dispensed with. According to Article 5, litra b, this can take place when the data subject consents, when there is authority in a national rule or in Community law, when legitimate interests of the data subject do not preclude it or

16. One example would be a hotel reservation transmitted electronically to a foreign country.

17. *See* NEW TECHNOLOGIES *supra* note 3, at 40-41.

18. The European Council, art. 5.

when it is necessary to ward off an imminent threat to public order or infringement of the rights of others. As it is impractical to get consent, the normal situation will call for an estimation of the interests of the data subject and whether any serious interests are challenged by a change of purpose. It is important that the evaluation is fairly strict.

One thing is registration; another, more important matter, is communication of recorded information. This issue is dealt with in Article 6. Distribution to another public authority can take place when it is necessary either for the communicating or requesting authority. An evaluation must determine whether the requirement of necessity has been met. Information can be communicated to the private sector if the interests favouring this communication prevail over the interests of the data subject. This is a very widely formulated rule and misuse can take place, which is the reason why additional guarantees have been instituted. The data subject must be notified about the communication unless it is stated in national legislation that a license from the data protection authority is sufficient. This possibility will probably be used by several countries, since having to inform data subjects is fairly impractical and can often be too expensive.

Concern with regard to communication is underlined in Article 7, which states that all files from which data might be communicated must be notified to the supervisory authority who must keep, in most cases, a publicly accessible file on these notifications. National legislation can determine precisely what the notification must contain, but at a minimum it must cover the identity of the authority maintaining the file, its purpose, a description of the data types, any third parties who might receive the information and the security measures taken to safeguard the information. This is one of the rules which illustrates the first generation approach. Although it is correct that communication of data can create risks for invasion of privacy, it must also be acknowledged that such a danger does not exist with respect to all kinds of data and that measures which are too bureaucratic can be a form of overkill leading to a situation where public authorities cannot reasonably benefit from the advantages of data technology. It is not necessary to insist that all files be notified. It would be better to restrict this demand to files containing sensitive information (as described in Article 17 discussed below) and perhaps files specifically mentioned in national legislation.

One subject is missing in these rules and in the directive in general. This is the question of matching files. For many years matching has been viewed as a most dangerous procedure and it is quite strange that the directive is silent on this point. Matching can be seen as a qualified form of communication for which special control mechanisms should be implemented. It is commonly recognized that combining files creates

certain risks with respect to data quality since data is collected at different times and for different purposes and that such combination of data can also provide public authorities with too comprehensive a picture of the individual citizen. Until recently there have been very strict rules on matching in Danish law, but this attitude has become somewhat liberalized today.[19] However, it is still recognized that matching with the purpose of subsequent control of citizens can be dangerous.

It could be stated in the directive either that matching for this purpose cannot take place, or maybe better still, that it presupposes prior authorization by the supervisory authority. Regardless of how matching is viewed, it is strange that this procedure is omitted in a directive which aims at providing a high level of protection.

2. *Private Sector*

For the private sector substantial rules are laid down in Article 8. There are three grounds for the legal recording of personal information. First, it can be due to a contract or a quasi-contractual relationship with the data subject. It will only be in a minority of cases where such circumstances exist, although this depends on how strict the concept of quasi-contractual relationships is viewed.

Second, publicly accessible information can be recorded when it is only used for correspondence. As this purpose is limited, this seems to be fairly unproblematic.

Third, information can be recorded when "the controller of the file is pursuing a legitimate interest" over which the interests of the data subject do not prevail. This is, of course, a very open condition and it is important to ensure that in practice this rule does not give way to extensive filings. In national legislation specific conditions for registration within the framework of the directive should be stated.

The rules on communication of recorded information refer to national legislation, where rules must be stated to prevent communication contrary to the purpose of the file. When a file is used on-line the same obligation is imposed on the user. This rather unclear rule means that the possibilities of communication are more limited in the private sector than in the public sector where a change of purpose is possible. Depending on how precise the purpose is laid down, situations can occur where this rule is very bureaucratic.

An information procedure for use in connection with the communication of data is provided in Article 9. The first time that data is communicated or there is an opportunity for on-line consultation, the data subject must be informed of the purpose of the file, the types of stored

19. In June 1990 a special act concerning control of public payments was passed by Parliament. This act provides authority for the matching of many public files.

data and the location of the file. This information is not necessary when the file contains public accessible data or the communication is required by law. If the data subject protests about the communication it should cease unless authorized by law. Although Article 10 provides that national legislation may derogate the demand of information to the data subject through authorization by the supervisory authority, it is clear that communication of recorded data is viewed very strictly and it seems doubtful that such severe rules are necessary. They are rather impractical and will probably create major difficulties for private enterprises.

This impression is strengthened by Article 11 which states that the creation of a file from which information not publicly accessible is to be communicated must be notified to the supervisory authority. If the file is located in a third country, notification should be made in the member country where the controller of the file resides. The notification should contain the same kind of information as in the public sector, as discussed above. Since manually processed files are also covered by the directive, this is a very far-reaching rule from which there are no exemptions. This will create a very bureaucratic system with the risk that data protection in general will be discredited.

It must be understood that a condition for the efficiency of these rules is that they are respected by the controllers of files and data users. Accordingly, measures that are too bureaucratic and that also presuppose large public expenditures should be avoided. In my opinion the notification rule is too severe and inflexible.

3. *Sensitive Data*

The question of special rules for sensitive data has been mentioned above, and Article 17 contains rules concerning the automatic processing of such data.[20] From the outset the recording of such information is prohibited unless the data subject has freely given an express, written consent. While it is recognized that consent is often a weak form of data protection, in many situations a prohibition on recording sensitive data will be contrary to important social goals and therefore, the member states have the authority to derogate this rule, provided such provisions are clear and specified.

Data concerning criminal convictions, however, can only be stored in public sector files. Since the reasons for data protection are extremely clear for this kind of data, Article 17 must be supported. It is,

20. The rule mentions "data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs or trade-union membership, and of data concerning health or sexual life."

however, not clear why manual files are not included, since the privacy interests are just as strong with respect to such files.

D. Quality and Security

In addition to the rules on filing and communication there are rules in Articles 16 and 18 concerning data quality and data security. In particular the rules on security are interesting since, among other things, they state that the member states shall take into consideration recommendations from the Commission on security and network interoperability. It is clear that in practice many data protection rules are dependent upon efficient security measures to ensure that unauthorized access in all its different forms does not take place. It is also clear that such security measures are particularly important with respect to computerized files where the possibility of such access is more varied than in the case of manual records.

It must also be emphasized, however, that although the demand for security should be strict it should not be exaggerated. In Danish law the demands for security are graduated depending on the sensitivity of the files. This approach is also taken in the directive. In Denmark as in many countries there has been friction between data users and the supervisory authority concerning how security should be organized.[21] Security measures should give sufficient protection to data files without making it impossible to access and use those files for other acceptable purposes.

If security measures differ substantially between the member countries, these differences may limit the free flow of data between them, and thereby undermine the rationale of the directive. This is, of course, the reason why the Commission is given a say in this matter, and this factor also clearly links the directive to the above-mentioned action plan for information security.

E. Citizen's Rights

Whether recorded information is correct and whether filing and communication affect integrity are issues that will differ from person to person. Considering that the rules are made for the protection of citizens, it is important that citizens be provided with certain rights. These rights are outlined in Articles 12-15.

As mentioned above, many of the substantive rules are based upon the consent of the data subject, and accordingly, it is important to deter-

21. In particular, security measures for personal computers have been debated. In principle, security demands should be the same regardless of which kind of data system is used, but, for example, a demand of logging data has created many problems when PCs are used.

mine which conditions must be fulfilled for a valid consent. This issue is covered in Article 12 where the principle of informed consent is outlined. The data subject must know the identity and purpose of the file, the types of data collected, the types of use to be made of the data and possible recipients. With this background a consent must be specified and expressed and can be withdrawn at any time. It is well-known that consent can be a doubtful method of ensuring data protection and not always given voluntarily or with an understanding of the consequences. It is therefore necessary, as done in Article 12, to set up criteria for valid consents, but it is still important to have a clear understanding of the limitations of this form of legal guarantee.

Article 13 states the minimum information a data subject should be given when required to provide data about himself. The main types of information are the following:

1. The purpose of the file for which information is wanted. It is important for the purpose to be explained clearly and precisely.

2. Whether a reply is obligatory or voluntary and what consequences attach to a failure to reply. As the tendency to gather vast amounts of information is widespread, it is important for citizens to know the authority for information gathering so that they are not lured into providing information they are not required to deliver.

3. For whom is the information intended, and

4. That they have a right of access and right of correction with respect to the stored information.

There will be certain files where all this information will prevent the exercise of important public tasks and such files are accordingly exempt from these demands.

In Article 14 data subjects are given several additional rights. The eight rights outlined below are from different perspectives both interesting and important.

1. A citizen has the right for legitimate reasons to oppose the processing of his data. In an information society such a right of rejection is essential for citizens, but the efficiency of this rule depends upon how legitimacy is defined and practice will thus be decisive.

2. A decision involving an assessment of the conduct of the data subject cannot be based solely on automatic processing of personal data. Seen from the perspective of computer law, this is probably the most interesting rule because it reaches developments within artificial intelligence. Among other things attempts to develop expert systems aim at making it possible to

make fully automated decisions. This is also the case to a certain degree with many of the not-so-advanced computer systems already in use. It seems clear that this rule will restrict the use of such systems. This rule is based upon the notion that citizens should have some ability to control decisions concerning themselves and that such a principle is more important than the administrative benefits of the most advanced parts of modern computer technology.

3. The data subject must know the existence of the file, its purpose and location. There should not be any secret gathering of information. Such a principle of openness is essential in democratic societies. It is secrecy that has been emphasized as one of the greatest threats to modern society.

4. The data subject must have a right of access within a reasonable interval. It has often been stated that access is the foremost right of citizens in connection with data protection, and, in principle, this is correct. International experience, however, shows that this right is not exercised by many citizens. As access is the best way to ensure high data quality, this is a disturbing experience and should not be viewed as an indication of satisfaction with the use of personal data. It is important that citizens are informed fairly regularly about their right of access.

5. The data subject can demand to have information that has been processed in violation of the directive erased, rectified or blocked. This provision concerns both unlawful and incorrect information. From the perspective of both data subjects and data users incorrect or misleading data should be corrected. In practice this provision ought not give rise to major disputes.

6. Data subjects have the right to request that information held in files for market research or advertising be erased. This rule concerns correct data, but it is recognized that citizens should not be obliged to have their information used for such purposes. As we are all constantly affected by marketing activities, and as many citizens find this disturbing, this right of erasure is of major practical importance.

7. If data has been corrected, third parties who received the erroneous information should be notified about the measures taken. This rule places certain obligations on controllers of files. They must be aware of whom information is communicated to and know the identity of the receivers. As the rule contains no time limits, this can be a burdensome responsibil-

ity. Consideration should be given to limiting this right to information that has been communicated within the last six months.[22]

8. Finally, data subjects should be able to pursue their rights with judicial remedies. This means that an administrative procedure which precludes access to the courts cannot be imposed. On the other hand, the supervisory authority should be the main source of help for data subjects in exercising their rights. This is easier for citizens than using the courts.

The rights of data subjects are many and varied. Exercise of one of these rights, access, can in some situations lead to files not being able to serve their legitimate purpose. This is particularly true in the public sector and Article 14 permits statutory limits on access and the right to know the existence of files if one of seven specified reasons exist, including national security and public safety. In these situations the supervisory authority on request can inspect the contents of the file on behalf of the data subject. This is very important since it would be dangerous if files could exist with no external control over data quality possible.

It is the right of access which can be limited, and only very seldom the right to know the existence of files. Seen from the perspective of democracy it is disturbing that files can exist which are not known to citizens.

F. Data Exports to Third Countries

A main purpose of the directive is to provide for free data flow between the member states. It is clear, however, that to a large extent data is exchanged between these states and third countries, including the United States.[23] Accordingly, it is important to determine under which circumstances such data traffic can take place. This is a politically sensitive question as strict rules can foster accusations that the EEC is creating a "fortress Europe." On the other hand, the high level of protection in the directive means that such data traffic cannot take place without certain guarantees. The problems are dealt with in Articles 24 and 25. It is likely that these two rules will be the object of lobbying from multinational firms during the negotiations before the final directive is issued.

The rules are based upon the principle of *equivalence*. Article 24 states that data can only be transferred to a country that "ensures an

22. For example, this is the rule in section 14 of the Danish Data Protection Act for the private sector concerning credit rating agencies.

23. Approximately twenty-five percent of all European data transactions are with the United States. See H. COLLIER *supra* note 4, at 3.

adequate level of protection." In practice this means that third countries must have data protection legislation that covers both the public and the private sector—a condition that many countries fail to fulfill. The Commission will make a list of the countries which fulfill the requirements. It will be important whether the country has ratified the European Data Convention. If, as proposed, the EEC as such adheres to the Convention, ratification is expected to be decisive.

If a country is not on the list, the member state has an obligation to ensure that an adequate level of protection exists and, when this is not found to be the case, to inform the Commission which can open negotiations with the country in question. It seems fairly clear that Article 24 will create problems with respect to transatlantic data flow. It may become a major incentive for the United States to enact comprehensive federal data protection legislation covering both the public and private sectors.

Despite the fact that Article 24 affects the ability of multinational businesses to operate, this rule is necessary for the legal protection of citizens. It also is clear that it is necessary to reach a global understanding of how data protection should be organized. This is discussed below.

Even when a country does not fulfill the conditions outlined in Article 24 in general, Article 25 permits a country to allow singular data exports when there is "sufficient proof that an adequate level of protection will be provided." This, however, presupposes that the other member countries and the Commission are informed and allowed a 10-day period for stating objections. If the proposed export meets those objections, the Commission can prohibit it.

A possible method of applying Article 25 could be by contract. A contractual relationship could be established between the exporting and importing agency, and this contract could be submitted for approval by the supervisory authority in the exporting country. There are several difficult legal problems attached to the use of contracts in this area.[24] Among other things it is doubtful how the rights of the data subjects who are not parties to the contract can be ensured. While the use of contracts cannot be ruled out, in general it must be recognized that this is not an adequate method and should be applied with caution. However, before an international regulation is fully developed contracts will sometimes be the only method to make singular data export possible. This issue is discussed further in the next section.

---

24. The question is discussed by Napier, in INT'L COMPUTER L. ADVISER, Vol. 4, No. 12, at 8-19.

G. CONTROL

Two major problems with data protection is how to control it in practice and how to keep the rules up to date. Article 26 states that all countries must have an independent supervisory authority with powers to enforce the national rules according to the directive. Today countries with data protection legislation have an administrative authority, but the important part of Article 26 is that the authority must be independent, i.e., not under instructions from the government, which seems to be necessary when public files are also to be controlled. In this connection it must be stressed that sufficient resources should be allocated to the authority to make it possible for it to employ personnel with computer expertise.

National control is not enough to ensure that the directive will function in accordance with its purpose. Accordingly, institutions will be set up at the EEC level to assist the Commission. The first is an independent "Working Party on the Protection of Personal Data," consisting of representatives of the supervisory authorities. The tasks of the Working Party are outlined in Article 28. It is particularly important that the Working Party contribute to the uniform application of the directive by comparing practice in different countries. It is well-known that even when two statutes look alike, practice can differ substantially and, in the last resort, it is practice that is important. Another task is to draft recommendations to the Commission concerning developments which should lead to new rules.

Article 30 creates an advisory committee composed of representatives from the various countries. This committee is to discuss proposals by the Commission concerning either security measures or new substantive rules. This should be viewed in conjunction with Article 29 where the Commission is given rule-making powers. The need for constant supervision of data protection regulations is taken seriously in the directive. It is these rules that make it feasible that the directive will have a significant effect.

H. CODES OF CONDUCT

Formulating data protection rules is difficult to do with sufficient precision. Many rules have to be quite broad. It is necessary that data users actively support these rules. Article 20 requests the member states to encourage business circles within different sectors to draw up European codes of conduct (ethical rules) having as their basis the rules of the directive. Such codes of conduct can play a major role as they may be felt more binding than the directive since they determine which firms are acting in an acceptable manner within a given sector. In relation to third countries these Codes of Conduct can generate a mutual

understanding which can sustain a tendency towards a broader international regulation.

I. IMPLEMENTATION

If the final directive is identical in principle to the draft described above, there will be a general high level of protection in Europe. The directive inevitably will influence legislation in other European countries since more countries will become members during the 1990s.

The directive will come into force on January 1, 1993, but will become effective when all countries have enacted or amended their national legislation. It seems realistic that the directive will not be effective before 1995. This is worth noting in connection with the problems attached to the relations between Europe and the rest of the world as discussed in the next section. However, the rules on data export to third countries will be effective in 1993, and accordingly, there is only a short time left to reach a global consensus on the appropriate level of data protection. The EEC can be the generator for such an understanding, which is probably the most important policy question in the coming years.

V. GLOBAL FLOW OF DATA

The information society knows no boundaries and embraces all developed countries. Politically and culturally the global exchange of data is of enormous importance. It is one of the best methods of developing international understanding and finally a more peaceful world. Accordingly, the interest in international data traffic is not exclusively linked to private enterprise and capital. There are overriding interests in ensuring such traffic. This is also true for personal data.

It must be recognized, however, that it is necessary to protect the privacy of individual citizens. It is important to develop a legal regulation which removes the threats that can follow from internationalization. A community such as the EEC where the member states have given some of their sovereignty to the common organization is most suitable to develop such rules, but this just makes it more necessary on a global level to find methods to establish binding international rules.

If such a goal is not achieved, data exchange on a global level will not be possible and there will be barriers both across the Atlantic and between Europe and the Pacific regions. It is important for computer lawyers to consider how this difficult problem can be solved.

The general solution is easy to envision but difficult to achieve. It must be a world convention, such as the conventions regulating intellectual property law. It is well-known that such a convention is very difficult to achieve and will take several years of negotiations. Even when

these difficulties are recognized, a world convention is necessary and it would seem likely that a strong EEC regulation will trigger such a convention. There is no doubt that such a convention will be a major step in the legal regulation and control of the information society. The central point in such a convention should be a rule determining when two national data protection laws can be deemed to be *equivalent*. The deciding point should be a regulation that is transparent to citizens and businesses but provides straightforward remedies when rules are violated.

With this background the first recommendation of this article is that efforts should be made for development of a world data convention, e.g., within the auspices of the United Nations. It will, take several years, however, before such a convention is finalized and consideration must be given to what to do in the interim. Experience shows that enactment of national legislation in this area is a slow process. Although more countries will have adequate rules in the future, there will still be major countries which do not have comprehensive legislation.

This means that the use of contracts must be seriously considered. This implies that each data exchange will be regulated separately, and although international model provisions could be developed, there will be some restraints on transborder data flow.

The major problems in using contracts that will only be backed by civil law remedies are in their drafting and enforcement. The contract must be between the exporting and importing firm, but it should be endorsed by the supervisory authority in the exporting country. The contract should state which data/files it covers, what use can be made of the data, who can access the data, the security measures to be taken and the rights of data subjects. The provisions should reflect an interest in a high level of data protection. The drafting of these substantial clauses should not present major problems.

It is more difficult to determine how the clauses can be controlled and sanctions imposed in case of a breach. As for control it seems best if a public authority in the importing country assumes this obligation. It is too difficult to perform controlling activities from abroad. Enforcement can probably best take place through arbitration in the exporting country whose national legislation should also be applied.

Finally, a question remains how the data subject, who is not a party to the contract, can acquire and enforce his rights without resorting to the law of a foreign country, which would be a major practical obstacle. It is probably best to make the exporting firm a kind of guarantor of those rights so that, for example, personal access can be achieved through this firm. Violations of the rules should also be the primary responsibility of the exporting firm.

There are many difficult legal problems attached to the use of contracts in this area. It can only be a temporary method before all countries have adequate legislation. Accordingly, the possibility of using contractual solutions should not slow efforts for a global consensus on data protection.

VI. EXCHANGE OF VIEWS

The international regulation of data protection is moving steadily towards common standards. The EEC directive will undoubtedly have a major influence on global regulation, but it is disturbing that, particularly in the private sector, a consensus does not exist on the level of protection. As data protection rules limit the use of data technology and influence the design of technical facilities both in hardware and software, it is unfortunate that the level of protection is so different. This is also unfortunate because new technological developments constantly create new data protection problems which should be solved in a similar way.

All these phenomena point to the need for a more intense exchange of views and not the least of which is an increased transatlantic discussion. It will be unacceptable in the long run if Europe and the U.S. follow different directions. Although traditions differ and the legal systems are quite different in the two regions, it should be possible to reach a common understanding in this area. This article is a small attempt to promote the transatlantic exchange of views. As a conclusion it is appropriate to express the hope that a true international regulation of data protection will be developed before the year 2000. This would be an appropriate manifestation of an aspiration to legally regulate the information society, so that citizens are offered satisfactory and secure legal protection.

Let data protection be an important part of the global *lex informatica*.

APPENDIX

PROPOSAL FOR A COUNCIL DIRECTIVE CONCERNING THE PROTECTION OF INDIVIDUALS IN RELATION TO THE PROCESSING OF PERSONAL DATA

COM(90) 314 final—SYN 287
(Submitted by the Commission on 27 July 1990)
(90/C277/03)

THE COUNCIL OF THE EUROPEAN COMMUNITIES.

Having regard to the Treaty establishing the European Economic Community, and in particular Articles 100A and 113 thereof,

Having regard to the proposal from the Commission,

In cooperation with the European Parliament,

Having regard to the opinion of the Economic and Social Committee,

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Single European Act, include establishing an even closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitutions and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas the establishment and the functioning of an internal market in which, in accordance with Article 8a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely, regardless of the Member States in which they are processed or requested, but also that fundamental rights should be safeguarded in view of the increasingly frequent recourse in the Community to the processing of personal data in the various spheres of economic and social activity;

(3) Whereas the internal market comprises an area without frontiers; whereas, for that reason, the national authorities in the various Member States are increasingly being called upon, by virtue of the operation of Community law, to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State;

(4) Whereas the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications net-

works in the Community necessitate; and facilitate cross-border flows of personal data;

(5) Whereas the difference in levels of protection of privacy in relation to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of out Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(6) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of privacy in relation to the processing of such data must be equivalent in all the Member States, whereas to that end it is necessary to approximate the relevant laws;

(7) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights, notably the right to privacy which is recognized both in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those 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;

(8) Whereas the principles underlying the protection of privacy in relation to the processing of personal data set forth in this Directive may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(9) Whereas the protection principles must apply to all data files where the activities of the controller of the file are governed by Community law; whereas public-sector files which are not governed by Community law should, as is provided for in the resolution of the representatives of the Governments of the Member States of the European Communities meeting within the Council of Europe, be subject to the same protection principles set forth in national laws; whereas, however, data files falling exclusively within the confines of the exercise of a natural person's right to privacy, such as personal address files, must be excluded;

(10) Whereas any processing of personal data in the Community should be carried out in accordance with the law of the Member State in which the data file is located so that individuals are not deprived of the protection to which they are entitled under this Directive;

whereas, in this connection, each part of a dam file divided among several Member States must be considered a separate data file and transfer to a non-member country must not be a bar to such protection;

(11) Whereas any processing of personal data must be lawful; whereas such lawfulness must be based on the consense of the data subject or on Community or national law;

(12) Whereas national laws may, under the conditions laid down in this Directive, specify rules on the lawfulness of processing: whereas, however, such a possibility cannot serve as a basis for supervision by a Member State other than the State in which the data file is located, the obligation on the part of the latter to ensure, in accordance with this Directive, the protection of privacy in relation to the processing of personal data being sufficient, under Community law, to permit the free flow of data;

(13) Whereas the procedures of notification, in respect of public or private sector data files, and provision of information at the time of first communication, in respect of private sector data files, are designed to ensure the transparency essential to the exercise by the data subject of the right of access to data relating to him;

(14) Whereas the data subject must, if his consent is to be valid and when data relating to him are collected from him, be given accurate and full information;

(15) Whereas the data subject must be able to exercise the right of access in order to verify the lawfulness of the processing of data relating to him and their quality;

(16) Whereas, if data are to be processed, they must fulfil certain requirements; whereas the processing of data which are capable by their very nature of infringing the right to privacy must be prohibited unless the data subject gives his explicit consent, whereas, however, on important public interest grounds, notably in relation to the medical profession, derogations may be granted on the basis of a law laying down precisely and strictly the conditions governing and limits to the processing of this type of data;

(17) Whereas the protection of privacy in relation to personal data requires that appropriate security measures be taken, both at the level of design and at that of the techniques of processing, to prevent any unauthorized processing;

(18) Whereas, as regards the media, the Member States may grant derogations from the provisions of this Directive in so far as they are designed to reconcile the right to privacy with the freedom of information and the right to receive and impart information, as guaranteed, in particular, in Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms;

(19) Whereas the Member States must encourage the drawing up, by the business circles concerned, of European codes of conduct or professional ethics relating to certain specific sectors; whereas the Commission will support such initiatives and will take them into account when it considers the appropriateness of new, specific measures in respect of certain sectors;

(20) Whereas, in the event of non-compliance with this Directive, liability in any action for damages must rest with the controller of the file; whereas dissuasive sanctions must be applied in order to ensure effective protection;

(21) Whereas it is also necessary that the transfer of personal data should be able to take place with third countries having an adequate level of protection; whereas, in the absence of such protection in third countries, this Directive provides, in particular, for negotiation procedures with those countries;

(22) Whereas the principles contained in this Directive give substance to and amplify those contained in the Council of Europe Conventions of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data;

(23) Whereas the existence in each Member State of an independent supervisory authority is an essential component of the protection of individuals in relation to the processing of personal data; whereas, at Community level, a Working Party on the Protection of Personal Data must be set up and he completely independent in the performance of its functions; whereas having regard to its specific nature it must advise the Commission and contribute to the uniform application of the national rules adopted pursuant to this Directive;

(24) Whereas the adoption of additional measures for applying the principles set forth in this Directive calls for the conferment of rule-making powers on the Commission and the establishment of an Advisory Committee in accordance with the procedures laid down in Council Decision 87/373/EEC[1],

---

1. OJ No I.197, 18.7 1987, p. 33.

HAS ADOPTED THIS DIRECTIVE:

CHAPTER I
GENERAL PROVISIONS

Article 1
Objective of the Directive

1. The Member States shall ensure, in accordance with this Directive, the protection of the privacy of individuals in relation to the processing of personal data contained in data files.

2. The Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons to do with the protection afforded under paragraph 1.

Article 2
Definitions

For the purposes of this Directive:

(a) "personal data" means any information relating to an identified or identifiable individual ("data subject"), an identifiable individual is notably an individual who can be identified by reference to an identification number or a similar identifying particular;

(b) "depersonalize" means modify personal data in such a way that the information they contain can no longer be associated with a specific individual or an individual capable of being determined except at the price of an excessive effort in terms of staff, expenditure and time;

(c) "personal data file" (file) means any set of personal data, whether centralized or geographically dispersed, undergoing automatic processing or which, although not undergoing automatic processing, are structured and accessible in an organized collection according to specific criteria in such a way as to facilitate their use or combination;

(d) "processing" means the following operations, whether or not performed by automated means: the recording, storage or combination of data, and their alteration, use or communication, including transmission, dissemination, retrieval, blocking and erasure;

(e) "controller of the file" means the natural or legal person, public authority, agency or other body competent under Community law or the national law of a Member State to decide what will be the purpose of the file, which categories of personal data will be stored, which operations will be applied to them and which third parties may have access to them;

(f) "Supervisory authority" means the independent public authority or other independent body designated by each Member State in accordance with Article 26 of this Directive;

(g) "public sector" means all the authorities, organizations and entities of a Member State that are governed by public law, with the exception of those which carry on an industrial or commercial activity, and bodies and entities governed by private law where they take part in the exercise of official authority;

(h) "private sector" means any natural or legal person or association, including public sector authorities, organizations and entities in so far as they carry on an industrial or commercial activity.

Article 3
Scope

1. The Member States shall apply this Directive to files in the public and private sectors with the exception of files in the public sector where the activities of that sector do not fall within the scope of Community law

2. This Directive shall not apply to files held by:

(a) an individual solely for private and personal purposes, or

(b) non-profit-making bodies, notably of a political, philosophical, religious, cultural, trade union, sporting or leisure nature, as part of their legitimate aims, on condition that they relate only to those members and corresponding members who have consented to being included therein and that they are not communicated to third parties.

Article 4
Law applicable

1. Each Member State shall apply this Directive to:

(a) all files located in its territory;

(b) the controller of a file resident in its territory who uses from its territory a file located in a third country whose law does not provide an adequate level of protection, unless such use is only sporadic.

2. Each Member State shall apply Articles 5, 6, 8, 9, 10, 17, 18 and 21 of this Directive to a user consulting a file located in a third country from a terminal located in the territory of a Member State, unless such use is only sporadic.

3. Where a file is moved temporarily from one Member State to another, the latter shall place no obstacle in the way and shall not require

the completion of any formalities over and above those applicable in the Member State in which the file is normally located.

CHAPTER II
LAWFULNESS OF PROCESSING IN THE PUBLIC SECTOR

Article 5
Principles

1. Subject to Article 6, the Member States shall, with respect to files in the public sector, provide in their law that:

(a) the creation of a file and any other processing of personal data shall be lawful in so far as they are necessary for the performance of the tasks of the public authority in control of the file;

(b) the processing of data for a purpose other than that for which the file was created shall be lawful if:

— the data subject consents thereto, or

— it is effected on the basis of Community law, or of a law, or a measure taken pursuant to a law, of a Member State conforming with this Directive which authorizes it and defines the limits thereto, or

— the legitimate interests of the data subject do not preclude such change of purpose, or

— it is necessary in order to ward off an imminent threat to public order or a serious infringement of the rights of others.

Article 6
Processing in the public sector having as its object the communication of personal data

1. The Member States shall provide in their law that the communication of personal data contained in the files of a public sector entity shall be lawful only if:

(a) it is necessary for the performance of the tasks of the public sector entity communicating or requesting communication of the data; or

(b) it is requested by a natural or legal person in the private sector who invokes a legitimate interest, on condition that the interest of the data subject does not prevail.

2. Without prejudice to paragraph 1, the Member States may specify the conditions under which the communication of personal data is lawful.

3. The Member States shall provide in their law that, in the circumstances referred to in paragraph 1(b), the controller of the file shall in-

form data subjects of the communication of personal data. The Member States may provide for the replacing of such provision of information by prior authorization by the supervisory authority.

Article 7
Obligation to notify the supervisory authority

1. The Member States shall provide in their law that the creation of a public sector file, the personal data in which might be communicated, shall be notified in advance to the supervisory authority and recorded in a register kept by that authority. The register shall be freely available for consultation.

2. The Member States shall specify the information which must be notified to the supervisory authority. That information shall include at least the name and address of the controller of the file, the purpose of the file, a description of the types of data it contains, the third parties to whom the data might be communicated and a description of the measures taken pursuant to Article 18.

3. The Member States may provide that paragraphs 1 and 2 shall apply to other public sector files and that consultation of the register may be restricted for the reasons stated in Article 15(1).

CHAPTER III
LAWFULNESS OF PROCESSING
IN THE PRIVATE SECTOR

Article 8
Principles

1. The Member States shall provide in their law that, without the consent of the data subject, the recording in a file and any other processing of personal data shall be lawful only if it is effected in accordance with this Directive and if:

(a) the processing is carried out under a contract, or in the context of a quasi-contractual relationship of trust, with the data subject and is necessary for its discharge; or

(b) the data come from sources generally accessible to the public and their processing is intended solely for correspondence purposes, or

(c) the controller of the file is pursuing a legitimate interest, on condition that the interest of the data subject does not prevail.

2. The Member States shall provide in their law that it shall be for the controller of the file to ensure that no communication is incompatible with the purpose of the file or is contrary to public policy. In the event

of on-line consultation, the same obligations shall be incumbent on the user.

3. Without prejudice to paragraph 1, the Member States may specify the conditions under which the processing of personal data is lawful.

Article 9
Obligation to inform the data subject

1. The Member States shall, with respect to the private sector, provide in their law that at the time of first communication or of the affording of an opportunity for on-line consultation the controller of the file shall inform the data subject accordingly, indicating also the purpose of the file, the types of data stored therein and his name and address.

2. The provision of information under paragraph 1 shall not be mandatory in the circumstances referred to in Article 8(1)(b). There shall be no obligation to inform where communication is required by law.

3. If the data subject objects to communication or any other processing, the controller of the file shall cease the processing objected to unless he is authorized by law to carry it out.

Article 10
Special exceptions to the obligation to inform the data subject

If the provision of information to the data subject provided for in Article 9(1) proves impossible or involves a disproportionate effort, or comes up against the overriding legitimate interests of the controller of the file or a similar interest of a third party, the Member States may provide is their law that the supervisory authority may authorize a derogation.

Article 11
Obligation to notify the supervisory authority

1. The Member States shall provide in their law that the controller of the file shall notify the creation of a personal data file where the data are intended to be communicated and do not come from sources generally accessible in the public. The notification shall be made to the supervisory authority of the Member State in which the file is located or, if it is not located in a Member State, to the supervisory authority of the Member State in which the controller of the file resides. The controller of the file shall notify to the competent national authorities any change in the purpose of the file or any change in his address.

2. The Member States shall specify the information which must be notified to the supervisory authority. That information shall include at least the name and address of the controller of the file, the purpose of the file, a description of the types of data it contains, the third parties to whom the data might be communicated and a description of the measures taken pursuant to Article 18.

3. The Member States may provide that paragraphs 1 and 2 shall apply to other private sector files and that the information referred to in paragraph 2 shall be accessible to the public.

CHAPTER IV
RIGHTS OF DATA SUBJECTS

Article 12
Informed consent

Any giving of consent by a data subject to the processing of personal data relating to him within the meaning of this Directive shall be valid only if:

(a) the data subject is supplied with the following information:
- — the purposes of the file and the types of data stored,
- — the type of use and, where appropriate, the recipients of the personal data contained in the file,
- — the name and address of the controller of the file;

(b) it is specific and express and specifics the types of data, forms of processing and potential recipients covered by it;

(c) it may be withdrawn by the data subject at any time without retroactive effect.

Article 13
Provision of information at the time of collection

1. The Member States shall guarantee individuals from whom personal data are collected the right to be informed at least about:

(a) the purposes of the file for which the information is intended;

(b) the obligatory or voluntary nature of their reply to the questions to which answers are sought;

(c) the consequences if they fail to reply;

(d) the recipients of the information;

(e) the existence of the right of access to and rectification of the data relating to them; and

(f) the name and address of the controller of the file.

2. Paragraph 1 shall not apply to the collection of information where to inform the data subject would prevent the exercise of the supervision and verification functions of a public authority or the maintenance of public order.

Article 14
Additional rights of data subjects

The Member States shall grant a data subject the following rights:

1. To oppose, for legitimate reasons, the processing of personal data relating to him.
2. Not to be subject to an administrative or private decision involving an assessment of his conduct which has as its sole basis the automatic processing of personal data defining his profile or personality.
3. To know of the existence of a file and to know its main purposes and the identity and habitual residence, headquarters or place of business of the controller of the file.
4. To obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in a file and communication to him of such data in an intelligible form.

   The Member States may provide that the right of access to medical data may be exercised only through a doctor.
5. To obtain, as the case may be, rectification, erasure or blocking of such data if they have been processed in violation of the provisions of this Directive.
6. To obtain upon request and free of charge the erasure of data relating to him held in files used for market research or advertising purposes.
7. To obtain, in the event of the application of paragraph 5 and if the data have been communicated to third parties, notification to the latter of the rectification, erasure or blocking.
8. To have a judicial remedy if the rights guaranteed in this Article are infringed,

Article 15
Exceptions to the data subject's right of access to public sector files

1. The Member States may limit by statute the rights provided for in points 3 and 4 of Article 14 for reasons relating to:

(a) national security;

(b) defense;

(c) criminal proceedings;

(d) public safety;

(e) a duly established paramount economic and financial interest of a Member State or of the European Communities;

(f) the need for the public authorities to perform monitoring or inspection functions; or

(g) an equivalent right of another individual and the rights and freedoms of others.

2. In the circumstances referred to in paragraph 1, the supervisory authority shall be empowered to carry out, at the request of the data subject, the necessary checks on the file.

3. The Member States may place limits on the data subject's right of access to data compiled temporarily for the purpose of extracting statistical information therefrom.

CHAPTER V
DATA QUALITY

Article 16
Principles

1. The Member States shall provide that personal data shall be:

(a) collected and processed fairly and lawfully;

(b) stored for specified, explicit and lawful purposes and used in a way compatible with those purposes;

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

(d) accurate and, if necessary, kept up to date; inaccurate or incomplete data shall be erased or rectified;

(e) kept in a form which permits identification of the data subjects for no longer than is necessary for the purpose for which the data re stored.

2. It shall be for the controller of the file to ensure that paragraph 1 is complied with.

Article 17
Special categories of data

1. The Member States shall prohibit the automatic processing of data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs or trade union membership, and of data concerning

health or sexual life, without the express and written consent, freely given, of the data subject.

2. The Member States may, on important public interest grounds, grant derogations from paragraph 1 on the basis of a law specifying the types of data which may be stored and the persons who may have access to the file and providing suitable safeguards against abuse and unauthorized access.

3. Data concerning criminal convictions shall be held only in public sector files.

Article 18

Data Security

1. The Member States shall provide in their law that the controller of a file shall take appropriate technical and organizational measures to protect personal data stored in the file against accidental or unauthorized destruction or accidental loss and against unauthorized access, modification or other processing.

Such measures shall ensure, in respect of automated files, an appropriate level of security having regard to the state of the art in this field, the cost of taking the measures, the nature of the data to be protected and the assessment of the potential risks. To that end, the controller of the file shall take into consideration any recommendations on data security and network interoperability formulated by the Commission in accordance with the procedure provided for in Article 29.

2. Methods guaranteeing adequate security shall be chosen for the transmission of personal data in a network.

3. In the event of on-line consultation, the hardware and software shall be designed in such a way that the consultation takes place within the limits of the authorization granted by the controller of the file.

4. The obligations referred to in paragraphs 1, 2 and 3 shall also be incumbent on persons who, either *de facto* or by contract, control the operations relating to a file.

5. Any person who in the course of his work has access to information contained in files shall not communicate it to third parties without the agreement of the controller of the file.

CHAPTER VI

PROVISIONS SPECIFICALLY RELATING TO CERTAIN SECTORS

Article 19

The Member States may grant, in respect of the press and the audiovisual media, derogations from the provisions of this Directive in so far as

they are necessary to reconcile the right to privacy with the rules governing freedom of information and of the press.

Article 20

The Member States shall encourage the business circles concerned to participate in drawing up European codes of conduct or professional ethics in respect of certain sectors on the basis of the principles set forth in this Directive.

CHAPTER VII
LIABILITY AND SANCTIONS

Article 21
Liability

1. The Member States shall provide in their law that any individual whose personal data have been stored in a file and who suffers damage as a result of processing or of any act incompatible with this Directive shall be entitled to compensation from the controller of the file.

2. The Member States may provide that the controller of the file shall not be liable for any damage resulting from the loss or destruction of data or from unauthorized access if he proves that he has taken appropriate measures to fulfil the requirements of Articles 18 and 22.

Article 22
Processing on behalf of the controller of the file

1. The Member States shall provide in their law that the controller of the file must, where processing is carried out on his behalf, ensure that the necessary security and organizational measures are taken and choose a person or enterprise who provides sufficient guarantees in that respect.

2. Any person who collects or processes personal data on behalf of the controller of the file shall fulfil the obligations provided for in Article 16 and 18 of this Directive.

3. The contract shall be in writing and shall stipulate, in particular, that the personal data may be divulged by the person providing the service or his employees only with the agreement of the controller of the file.

Article 23
Sanctions

Each Member State shall make provision in its law for the application of dissuasive sanctions in order to ensure compliance with the measures taken pursuant to this Directive.

CHAPTER VIII
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 24
Principles

1. The Member States shall provide in their law that the transfer to a third country, whether temporary or permanent, of personal data which are undergoing processing or which have been gathered with a view to processing may take place only if that country ensures an adequate level of protection.

2. The Member States shall inform the Commission of cases in which an importing third country does not ensure an adequate level of protection.

3. Where the Commission finds, either on the basis of information supplied by Member States or on the basis of other information, that a third country does not have an adequate level of protection and that the resulting situation is likely to harm the interests of the Community or of a Member State, it may enter into negotiations with a view to remedying the situation.

4. The Commission may decide, in accordance with the procedure laid down in Article 30(2) of this Directive, that a third country ensures an adequate level of protection by reason of the international commitments it has entered into or of its domestic law.

5. Measures taken pursuant to this Article shall be in keeping with the obligations incumbent on the Community by virtue of international agreements, both bilateral and multilateral, governing the protection of individuals in relation to the automatic processing of personal data.

Article 25
Derogation

1. A Member State may derogate from Article 24(1) in respect of a given export on submission by the controller of the file of sufficient proof that an adequate level of protection will be provided. The Member State may grant a derogation only after it has informed the Commission and the Member States thereof and in the absence of notice of

opposition given by a Member State or the Commission within a period of 10 days.

2. Where notice of opposition is given, the Commission shall adopt appropriate measures in accordance with the procedure laid down in Article 30(2).

CHAPTER IX
SUPERVISORY AUTHORITIES AND WORKING PARTY ON THE PROTECTION OF PERSONAL DATA

Article 26
Supervisory authority

1. The Member States shall ensure that an independent competent authority supervises the protection of personal data. The authority shall monitor the application of the national measures taken pursuant to this Directive and perform all the functions that are entrusted to it by this Directive.

2. The authority shall have investigative powers and effective powers of intervention against the creation and exploitation of files which do not conform with this Directive To that end, it shall have *inter alia* the right of access to files covered by this Directive and shall be given the power to gather all the information necessary for the performance of its supervisory duties.

3. Complaints in connection with the protection of individuals in relation to personal data may be lodged with the authority by any individual.

Article 27
Working Party on the Protection of Personal Data

1. A Working Party on the Protection of Personal Data is hereby set up. The Working Party, which shall have advisory status and shall act independently, shall be composed of representatives of the supervisory authorities provided for in Article 26 of all the Member States and shall be chaired by a representative of the Commission.

2. The secretariat of the Working Party on the Protection of Personal Data shall be provided by the Commission's departments.

3. The Working Party on the Protection of Personal Data shall adopt its own rules of procedure.

4. The Working Party on the Protection of Personal Data shall examine questions placed on the agenda by its chairman, either on his own initiative or at the reasoned request of a representative of the su-

pervisory authorities, concerning the application of the provisions of Community law on the protection of personal data.

Article 28
Tasks of the Working Party on the Protection of Personal Data

1. The Working Party on the Protection of Personal Data shall:

(a) contribute to the uniform application of the national rules adopted pursuant to this Directive;

(b) give an opinion on the level of protection in the Community and in third countries,

(c) advise the Commission on any draft additional or specific measures to be taken to safeguard the protection of privacy.

2. If the Working Party on the Protection of Personal Data finds that significant divergences are arising between the laws or practices of the Member States in relation to the protection of personal data which might affect the equivalence of protection in the Community, it shall inform the Commission accordingly.

3. The Working Party on the Protection of Personal Data may formulate recommendations on any questions concerning the protection of individuals in relation to personal data in the Community. The recommendations shall be recorded in the minutes and may be transmitted to the Advisory Committee referred to in Article 30. The Commission shall inform the Working Party on the Protection of Personal Data of the action it has taken in response to the recommendations.

4. The Working Party on the Protection of Personal Data shall draw up an annual report on the situation regarding the protection of individuals in relation to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission.

CHAPTER X
RULE-MAKING POWERS OF THE COMMISSION

Article 29
Exercise of rule-making powers

The Commission shall, in accordance with the procedure laid down in Article 30(2), adopt such technical measures as are necessary to apply this Directive to the specific characteristics of certain sectors having regard to the state of the art in this field and to the codes of conduct.

Article 30
Advisory Committee

1. The Commission shall be assisted by a Committee of an advisory nature composed of the representatives of the Member States and chaired by a representative of the Commission.

2. The representative of the Commission shall submit to the Committee of draft of the measures to be taken. The Committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter, if necessary by taking a vote. The opinion shall be recorded in the minutes; in addition, each Member State shall have the right to ask to have its position recorded in the minutes. The Commission shall take the utmost account of the opinion delivered by the Committee. It shall inform the Committee of the manner in which its opinion has been taken into account.

FINAL PROVISIONS

Article 31

1. The Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive by 1 January 1993. The provisions adopted pursuant to the first subparagraph shall make express reference to this Directive.

2. The Member States shall communicate to the Commission the texts of the provisions of national law which they adopt in the field covered by the Directive.

Article 32

The Commission shall report to the Council and the European Parliament at regular intervals on the Implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments.

Article 33

This Directive is addressed to the Member States.