Explanatory Memorandum
Recommendation No.R (91) 10 of the Committee of Ministers to Member States on the communication to third parties of personal data held by public bodies

(Adopted by the Committee of Ministers on 9 September 1991 at the 461st meeting of the Ministers' Deputies)

Preamble - The issues explained

1. "Greater unity between its members" - the aim of the Council of Europe - may be furthered in a range of different ways. Article 1 of the Statute of the Organisation makes specific reference to the Council of Europe's mission in maintaining and promoting human rights and fundamental freedoms as a way of achieving this "greater unity".

2. This recommendation falls squarely within this role. It is a human rights instrument. It is concerned with the circulation of information within society and at the same time with the protection of the private life of the individual. In other words, Article 8 (the right to private life) and Article 10 (freedom of expression) of the European Convention on Human Rights underlie the approach which motivates the various principles contained in the recommendation.

3. It is against this human rights background that references are made in the preamble to certain key legal instruments adopted by the Committee of Ministers of the Council of Europe in the field of both general information policy as well as privacy policy: Recommendation No. R (81) 19, the Declaration of the Committee of Ministers of 29 April 1982, the Data Protection Convention of 28 January 1981. All these legal instruments are designed to promote further (and reconcile) the fundamental freedoms spelt out in Articles 8 and 10 of the European Convention on Human Rights.

4. Freedom of information policy and privacy policy may compete for priority. The application of each of these fundamental values must be premised on respect for its counterpart. Reconciliation is sometimes necessary. This is why, for example, the implementation of freedom of information policy contained in Recommendation No. R (81) 19 is made subject to the need to respect, *inter alia,* the private life of the individual. From the privacy point of view, the implementation of data protection policy must, as is declared in the preamble to the Data Protection Convention, take account of the need "... to reconcile the fundamental values of respect for privacy and the free flow of information between peoples". For the intergovernmental Committee of Experts on Data Protection, the drafters of this legal instrument, freedom of information policy and data protection are not necessarily conflicting values. Data protection is to be seen as consistent with the broader aspects of information policy within society. It does not seek to place *a priori* restrictions on the circulation of personal information within society. Rather, the principles of data protection seek to determine the conditions under which personal data may be collected, processed and communicated to third parties, and used by them.

5. It should be stressed at the outset that the aim of this recommendation is not to promote transparency within public administration or open government or to encourage freedom of information. The desirability of making public bodies accountable by means of freedom of information principles is already catered for in Recommendation No. R (81) 19 of the Committee of Ministers.

The sort of principles advocated in Recommendation No. R (81) 19 are reflected in a number of national legal systems - for example, general laws on access to public sector information exist in Austria, Denmark, Finland, France, Greece, Netherlands, Norway and Sweden. Other countries envisage access to certain categories of public sector information. The drafters of this text are primarily concerned with the way in which the openness principle - whether in the context of a general law or a sectoral law - interacts with the protection to be accorded to the private life of the individual whose personal data may be communicated to third parties following an access request. Moreover, if personal information must be collected, stored and used by public bodies in accordance with general data protection policy and if, as noted earlier (paragraph 4), data protection policy does not block *a priori* the communication of personal data by public bodies to requesting third parties under access legislation, how are the conditions for communication to be determined?

6. Furthermore, a complete approach to personal data or personal data file communication by public bodies to third parties may not be limited solely to situations foreseen in provisions governing access to public sector information. The recommendation is also concerned with those many situations in which public bodies collect and store various categories of personal data with a view to their being made accessible to third parties in accordance with the whole range of legal provisions governing accessibility. In particular, the recommendation addresses those categories of so-called "public files" which contain personal data which are published in accordance with the law. Such files - examples are provided in paragraph 24 of this commentary - are available for public consultation and the data contained in them may be communicated to third parties.

7. The data protection concerns of the drafters of this recommendation are being expressed in the context of new trends in the handling of personal data or personal data files by public bodies - namely the electronic delivery of personal data or personal data files to requesting third parties, which has been made possible by virtue of the fact that data processing technology has allowed public bodies to store the data which they collect on electronic files. Given the fact that the interventionist and regulatory nature of public powers touches the lives of every citizen, it is not surprising that the databases held by public bodies contain massive quantities of personal information The richness of this information is, not surprisingly, of great interest to third parties, particularly commercial enterprises working within the private sector.

8. As the preamble notes, there is an increasing tendency on the part of the private sector to exploit personal data or personal data files held by public bodies in order to further marketing campaigns, plan economic strategy, target possible consumer populations,

enrich existing personal data files, etc. It is precisely the automation of personal data which facilitates their exploitation by third parties. The data may be accessed on-line, or public bodies may download electronically various categories of personal data files to third party databases. Print-outs of names and addresses in the form of automated labels may be sold by public bodies responsible for various types of public files. Alternatively, a third party may simply buy a magnetic tape containing particular personal data files.

9. It is interesting to note that the Commission of the European Communities has promulgated Guidelines which are designed to improve the synergy between the public and private sectors in the so-called "information market". The Guidelines, adopted in 1989, note the wealth of information at the disposal of public bodies and encourage its greater availability in the private sector:

"Public administrations regularly and systematically collect basic data and information in the performance of their governmental functions. These collections have value beyond their use by governments, and their wider availability would be beneficial both to the public sector and to private industry." (Principle 1 of the Guidelines.)

10. Of course, the policy advocated may be easily analysed in terms of freedom of information. It is quite compatible with, for example, Article 10 of the European Convention on Human Rights which is not simply limited to guaranteeing information circulation for the preservation and promotion of a democratic and pluralist society. The Declaration of the Committee of Ministers of 29 April 1982 notes, *inter alia,* that freedom of information and the right to seek and receive information are necessary for the social, economic, cultural and political development of every human being. However, as noted above, it is necessary to integrate data protection policy into this scheme of things whenever the information in question is of a personal nature. For the drafters of this recommendation, this is even more vital in view of the risks which electronic storage of personal information by public bodies, and its communication telematically to third parties may bring about, namely: electronic profiling of individual income, family situation, property ownership, indebtedness; the search for names in various disparate public files, the matching or interconnection of various pieces of personal information contained in those files; the use of data for purposes which did not motivate their collection and storage in a public file, etc.

In other words, the drafters of the recommendation have proceeded on the basis that the fact that personal data or personal data files are to be made accessible to third parties in accordance with "legal provisions" does not necessarily mean that they should not be protected from the point of view of data protection policy. This is in fact the primary purpose of the recommendation: to determine the conditions under which personal data may be collected and stored in such files and, in particular, the conditions under which these personal data may be communicated to, and used by, third parties.

11. In discussing the communication of personal data or personal data files by public bodies to third parties in the two situations described above - in accordance with provisions governing access to public sector information or in accordance with specific

legal provisions on publicity - the drafters of the recommendation are seeking to emphasise that a legal framework is essential before any communication may be effected. In so doing, they are seeking to avoid the existence of a grey zone, or a situation between law and non-law, wherein vague administrative practices or policies operate. It may be noted in passing that the sort of action which is proposed in this recommendation is consistent with the conclusions which emerged from the conference organised jointly between the Council of Europe and the Commission of the European Communities (Luxembourg, 27-28 March 1990) which dealt, *inter alia,* with the question of access to public sector information in the new automated environment.

Operative part - Sort of action which could be taken

12. As with the previous recommendations which it has elaborated for particular sectors, the Committee of Experts on Data Protection is once again offering a body of data protection principles for the benefit of national policy makers for a new context in which data processing technology has intervened to create new risks for the privacy of the individual. The principles contained in the appendix to the recommendation may in many ways be regarded as a counterpart to the Guidelines produced by the Commission of the European Communities for improving synergy between the public and private sectors in the information market. It is to be noted that these Guidelines alert public administrations to the need to protect "legitimate public or private interests" in implementing the policy outlined in the Guidelines. In addition to information to which access may be restricted for reasons of national security, external relations, commercial confidentiality, etc, the Guidelines also recognise that the protection of personal privacy and personal data is a legitimate reason for refusing to make available to third parties information held by public bodies. It is possible therefore to view the corpus of principles offered by the Committee of Experts on Data Protection as detailed guidance on how that need may be realised in practice by the governments of Community member states - as well as non Community members of course.

13. The importance of the role of national data protection authorities in applying these principles is also noted in the operative part of the recommendation. Some such authorities have already shown their readiness to place limitations on the use which may be made by public bodies of the personal data which they collect and which may be accessible to third parties. In addition, the recommendation also seeks to bring authorities established under provisions governing access to public sector information into the scheme of protection advocated in this recommendation. As is shown later in the text, a cross-fertilisation of the role of these agencies and the competence of data protection authorities is encouraged so as to ensure consistency of approach to the communication of personal data or personal data files by public bodies to third parties.

APPENDIX TO THE RECOMMENDATION

1. Scope and definitions

14. As noted in the preamble, the principles contained in the recommendation cover the totality of personal data which are collected by public bodies and which may be communicated to third parties. The text of Principle 1.1 avoids making any reference to the need for such data to be collected by public bodies in the discharge of their official functions. While it goes without saying that public bodies should only collect and store personal data for specific and lawful purposes linked to their authorised tasks, the drafters of the recommendation feel that it is worthwhile to include within its scope all personal data collected and held by public bodies which may be communicated to third parties.

15. Principle 1.1 emphasises that the recommendation is primarily concerned with personal data which are automatically processed by public bodies. This is consistent with the main concern which motivates the need for this recommendation, namely the electronic storage and communication of personal data to third parties by telematic means. Nevertheless, as noted in Principle 1.2, member states may extend the recommendation's principles to personal data which are held by public bodies in manual form. This flexibility is important since various categories of data held by public bodies may exist in both automated form as well as in hard copy. For example, the telephone directory - a personal data file for the purposes of this recommendation - exists both in hard copy form as well as in electronic form. It may also be noted in passing that the data protection legislation of a number of member states covers both automatic as well as manual processing.

16. Similarly, freedom to extend the scope of the recommendation applies to data concerning corporate bodies, groups, associations, etc, even though they do not possess legal personality in accordance with domestic company law. Much of the information held by public bodies concerns such entities. Reference may be made to files accessible to third parties such as companies' or commercial registers. This is an important factor to be borne in mind by policy makers whose data protection regimes cover both natural and legal persons, as well as any other body not possessing legal personality.

17. It may be noted that the possibilities for extending the scope of the recommendation described in Principle 1.2 are consistent with the provisions of Article 3, paragraph 2, sub-paragraphs *b* and *c,* of Convention No. 108.

18. Principle 1.3 is devoted to the definition of various critical terms which are used frequently throughout the recommendation.

19. The definition of "personal data" referred to in Principle 1.3 should not raise too many problems since the formula has been accepted by all member states in previous sectoral recommendations of the Committee of Ministers in the field of data protection. Policy-makers should pay particular attention to the issue of statistical data which, although held in non-nominate form, may nevertheless be linked, using sophisticated data

processing technology, to named individuals. The drafters of the present recommendation have noted that the Committee of Experts on Data Protection has recently embarked on work in the area of statistical data and it is expected that a separate legal instrument will be elaborated which will deal with the new problems arising out of the use, including communication, of statistical data held by public bodies.

20. It is of course the case that personal data may be put into circulation and made available to the public by private sector bodies. For example, traders may produce public registers containing the names and addresses of their members. Similarly, professional bodies in the private sector may bring out directories containing various degrees of personal information on their members - name, address, professional qualifications, their specialised fields, etc. However, this recommendation is only concerned with personal data handling by "public bodies". Such bodies perform public service or public interest activities. They may be found at state level or at the level of territorial communities. As opposed to private bodies, public bodies are amenable to principles of public law, in particular the possibility to seek judicial review of their administrative acts. There is of course a grey area between the activities of private bodies and public bodies. For example, it may be the case that certain bodies, linked budgetarily to the state or to territorial communities, compete in the market-place with private enterprises and under the same conditions as private enterprises. Moreover, private bodies may in certain countries perform public service or public interest activities. One has only to refer in this regard to privatised companies which, prior to deregulation policies, were legally and economically situated within the public sector.

21. While noting that it is possible to identify certain common criteria in all states for public bodies, the text admits that domestic law may take a more expansive view of the type of body which may be termed "public" for the purposes of the recommendation.

22. Principle 1.1, as noted earlier, is limited to those personal data which are collected by public bodies and "which may be communicated to third parties". The recommendation takes as its point of departure the need for communication of such data to be carried out on a legal basis. More often than not, such data will be contained in "files". The data should only be communicated to third parties if such files are in fact "accessible to third parties".

Principle 1.3, fourth sub-paragraph, identifies the various ways in which third parties may access personal data files and obtain communication of personal data stored in them. In the first place, files may be accessible to third parties in accordance with provisions governing access to public sector information or freedom of information. These provisions may be found in general laws governing freedom of information or access to public sector information. Alternatively, such provisions may be found in more limited legal contexts. In some countries, it may be the case that both general and sectoral access provisions exist. Other countries will only possess sectoral rules on access. As noted earlier, it is not the intention of the drafters to advocate general principles of access to public sector information or freedom of information or to adjust national law and procedure for granting access, or to harmonise the scope of legislation on openness. The

Committee of Ministers has already encouraged this action in Recommendation No. R (81) 19. The present recommendation is only concerned with addressing the new situation which has arisen since the automation of public sector databases and the possibilities which this has offered to third parties to have easier access to the nominate data contained in the databases without having to justify the reasons why they are seeking personal data files.

23. Moreover, files may be accessible to third parties. including the general public, because this was the intention of the legislator in specific enactments. These categories of files refer to the so-called "public files" which contain personal data which are collected and stored by public bodies with a view to their official publication. Although such files are generally accessible, it may be the case that access is limited to closed groups - for example certain states restrict access to files on criminal convictions to those operating within the criminal justice system. This "closed user group" restriction explains the reference in Principle 1.3, fourth sub-paragraph 4, to "third parties having a particular interest".

24. These "public files may include, in particular, telephone directories, electoral registers, land registers, files containing the names and addresses of consumers of electricity and gas, patent and trademark registers, files containing personal data relating to guardianship, commercial registers, vehicle-licensing registers, registers established by data protection authorities containing information on data users, etc. The recommendation proceeds on the basis that such public files must have been created in accordance with specific legal provisions. These may take the form of statutes, regulations, statutory instruments, etc. What is necessary is that the publication of information and its being made accessible to the public, including third parties, are mandated by law including, in the case of some countries, in accordance with provisions governing access to public sector information but, more commonly, in accordance with specific legal provisions governing public files.

25. There are many reasons why public files may come into existence. For example, they may be set up under statutes with a view to promoting the needs of transparency in a particular economic activity, typically the publication of the names of company directors. Again, information may be made public with a view to promoting public interest in various domains, for example the decision to make accessible to the public the names and addresses of those entitled to vote in national or local elections. Or, information may be made public so as to facilitate dealings between members of the public, as is the case with telephone directories. Finally, the interventionist nature of public powers leads to increased regulation of various activities. Regulation brings with it control over the persons involved in those activities - for example, through licensing procedures. It is not uncommon to find lists of licence-holders (data users, holders of firearm certificates, fishing permits, etc) published under statutory authority and thus made available to the public.

26. "Communication", a term which appears in the very title of the recommendation, is given a broad definition. It covers both bulk communication of personal data as well as

communication of isolated items of personal data contained in files accessible to third parties. The definition is intended to be technologically relevant. It covers communication by electronic or telematic means, electronic consultation by on-line methods as well as the physical delivery of magnetic tapes and electronic downloading of personal data or personal data files.

27. The "third parties" are defined so as to specifically exclude communication to public bodies. The definition obviously covers private sector companies, groups, associations, etc as well as individuals. The drafters of this recommendation have not dealt with the issue of communication of personal data or personal data files between public bodies whether for public interest purposes linked to their official functions or for other purposes such as marketing or economic planning outside the strict framework of such functions. As with the issue of statistical data discussed in paragraph 19, the drafters of the recommendation have noted that the Committee of Experts on Data Protection might look specifically at the issue of the communication of personal data between public bodies, with a view to elaborating a separate legal instrument.

28. Nevertheless, as noted in the course of the discussion, in the definition of "public bodies" a grey area may exist between the activities of public and private bodies, and different states may have different perceptions of what constitutes a private body and a public body. It is for this reason that the recommendation allows a certain flexibility in regard to the scope of the expression "third parties" by allowing states to broaden the scope of the expression "third parties" (Principle 1.3, seventh sub-paragraph).

2. Respect for privacy and data protection principles

29. The principles laid down in the recommendation are of course designed to ensure respect for the private life of the data subject when his data are to be communicated by public bodies to third parties. As such, the protective framework proposed in the body of the recommendation is consistent with the guarantees for privacy laid down in Article 8 of the European Convention on Human Rights. The drafters of the recommendation have also proceeded on the basis that the right to private life should be reinforced by reference to data protection principles which regulate the conditions in which personal data may be communicated and, in particular, the extent of involvement of the data subject in determining those conditions. In other words, the recommendation is more concerned with respect for privacy in terms of informational self-determination rather than in terms of a "right to be let alone". This view of privacy protection is better adapted to the new technological realities of personal data handling by public bodies as well as the new threats to individual privacy, autonomy, dignity and identity arising out of the misuse of personal data by technical means once the data have been communicated to third parties.

30. With these factors in mind, Principle 2 of the recommendation notes the need for safeguards and guarantees to accompany the communication of personal data or personal data files to third parties. Principle 2.1 stresses the need to make communication conditional on the existence of a legal basis authorising communication. To illustrate this, reference is made to specific laws, for example laws governing particular types of public

files; to freedom of information provisions, whether general or sectoral in nature; to authorisation granted under data protection legislation, including for example, the authorisation of an authority established under such legislation. All these different legal sources may constitute the basis for communication.

In the absence of such a legal basis, Principle 2.1.d states that the communication must be conditional on obtaining the "free and informed consent" of the data subject.

31. Principle 2.2 highlights the importance of continuing to respect the principle of purpose specification or finality after the stage of communication. The personal data collected by public bodies will have been collected for specific and lawful purposes linked to their official tasks. In accordance with Article 5, paragraph b, of Convention No. 108, the data so collected should not be used, including communicated, for other incompatible purposes. Principle 2.2 attempts to concretise the principle of purpose specification or finality in the sector covered by the recommendation. With this objective in mind, Principle 2.2 provides that personal data or personal data files may not be communicated to third parties for purposes incompatible with those for which the data were collected, unless appropriate safeguards and guarantees exist in domestic law. What may constitute "appropriate safeguards and guarantees" is discussed in paragraph 33. As regards the expression "domestic law", a broad interpretation may be given to this term. It may range from authorisation included in a statute, creating a particular public file, to a decision taken by a data protection authority or an agency set up under freedom of information legislation.

32. It is an accepted principle in many laws governing access to public sector information (one of the legal mechanisms to allow personal data files to be accessible to third parties) that the requesting third party need not justify the reasons why he seeks access to the data or to the data files, nor the purposes for which he will use them. Recommendation No. R (81) 19 of the Committee of Ministers also embodies the same principle of non-justification of an access request. Accordingly, in many countries where general laws on freedom of information or access to public sector information exist, public bodies may not restrict the communication of personal data to requesting third parties on the basis that the data sought will be used for incompatible purposes. This said, at the time of drafting this explanatory memorandum, some countries in Europe envisaged restricting the use of access to public sector information for the purpose of commercial exploitation of the data sought. The drafters of this recommendation feel that new trends towards storing personal data or personal data files in electronic form allowing them to be communicated telematically, including in bulk form, in accordance with provisions governing access to public sector information, require all states to review the uses which are being made of such laws. It may be the case that this new phenomenon was not in the minds of the drafters of such legislation when they sought to promote transparency within public administrations and the accountability of decision-makers.

33. As regards the sort of safeguards and guarantees which could be provided, reference may be made to such matters as the need to seek the free and informed consent of data subjects before the data are to be communicated for incompatible purposes, or at least to

inform them at the time of the collection of the data that these may be communicated to third parties for purposes other than those which motivated their collection, thus allowing them the possibility of raising an objection. These matters are dealt with in greater detail in Principles 4 et seq.

34. Principle 2.3 contains a general statement to the effect that the processing of the data by a third party after their communication is subjected to the requirements of domestic data protection legislation, including the procedural controls (notification, declaration, registration, etc of personal data files) exercised by the data protection authorities. Principle 6 gives further details on how data may be used by the third parties to whom they have been communicated. However, Principle 2.3 makes it quite clear that data protection legislation covers use as well as other processing stages, such as conservation of the data.

3. Sensitive data

35. The drafters of the recommendation have structured their approach to the issue of data communication in accordance with the nature of the data collected by public bodies. The nature of the data determines their accessibility to third parties and, accordingly, the conditions for their communication. This approach is reflected in the provisions of Principle 3 of the recommendation as well as in Principles 4 et seq. of the recommendation. Principle 3 relates to personal data which are generally non-accessible to third parties because of their sensitivity or their potential to prejudice the private life of data subjects if they were to be communicated to third parties. Principles 4 et seq, on the other hand, deal with personal data which are generally accessible in accordance with legal provisions. The nature of such data is different and, rather than blocking or taking an extremely restrictive approach to their communication, as with the type of data covered by Principle 3, the issue becomes one of determining the conditions under which such data may be communicated.

36. Principle 3.1 regards as "sensitive data" any of those categories of sensitive data which are referred to in Article 6 of Convention No. 108 (personal data revealing racial origin, political opinions, religious or other beliefs, personal data concerning health, sexual life or criminal convictions). It should be borne in mind that the list outlined in Article 6 is not exhaustive. Member states may have other perceptions of what constitutes personal data of a sensitive nature.

37. The general rule on sensitive data is clearly stated in Principle 3.1 - such data should not be placed in a file or in part of a file which is generally accessible to third parties. The drafters of the recommendation have recognised that such a general rule may not be absolute in nature. For example, in certain countries, lists of judgments in bankruptcy against certain individuals may be available for public consultation. Given that some of these countries may regard judgments in bankruptcy as criminal convictions, the list which is made accessible to third parties will contain one of the categories of sensitive data referred to in Article 6 of Convention No. 108. Moreover, the need to monitor the employment activities of enterprises in regard to their policy concerning the recruitment

of ethnic or religious minorities may give rise to the creation of files accessible to third parties which contain sensitive data. Nevertheless, given the fundamental nature of the safeguard stated in Principle 3.1, any exception to it may only be tolerated in well-defined circumstances laid down by law and accompanied by compensatory safeguards and guarantees. This is the purpose of the clause contained in the second sub-paragraph of Principle 3.1. In drafting this clause the drafters of the recommendation base themselves on the relevant derogations specified in Article 9 of Convention No. 108. For example, the two permissible exceptions referred to previously may be based on the provisions in Article 9 which refer to "the suppression of criminal offences" as well as "protecting the rights and freedoms of others". As regards the "appropriate safeguards and guarantees" referred to in the second sub-paragraph of Principle 3.1, the drafters had in mind the sort of safeguards referred to in Article 6 of the convention.

38. The reference to "stored in a file or in part of a file" is justified by reason of the fact that certain files which may be generally accessible may also contain personal data of a sensitive nature. The protective framework set out in Principle 3.1 would be seriously undermined if it did not deal with this possible lacuna.

39. Principle 3.2 is concerned with those situations in which public bodies hold lists of politicians' names and their political allegiance or lists of names of individuals who, although not politicians, are nevertheless involved in political life. For example, such individuals may be appointed to the private office of government ministers on the basis of their political affiliation. Of course, such data are *prima facie* sensitive since they fall within one of the categories set out in Article 6 of Convention No. 108.

40. Other types of situations not involving data concerning political beliefs may also be envisaged. For example, public bodies may hold lists of names of church leaders with indications on their particular religious affiliations. Once again, such data fall, *prima facie,* within Article 6 of Convention No. 108 since they relate to religious beliefs.

41. Nevertheless, the drafters of the recommendation believe that *prima facie* sensitive data in such circumstances may be made accessible to third parties since the data in question fall within "the public domain".

42. The drafters of this recommendation have come to this conclusion on the basis of an interpretation of Article 6 of Convention No. 108. In their view, such data concerning individuals involved in public life do not, within the strict meaning of the article, "reveal" such matters as political opinions or religious beliefs. In addition, the drafters of the recommendation believe that making data falling within the public domain accessible to third parties is also justified on the basis of Article 9, paragraph 2.*b*, of the Convention. It is felt that the accessibility of the data is justified as it is intended to contribute to open democracy and as such is for the protection of "the rights and freedoms of others".

43. In addition, in elaborating this provision, the drafters bore in mind the judgment of the European Court of Human Rights in the Lingens case in which the Court noted that, unlike a private individual, a politician "... inevitably and knowingly lays himself open to

close scrutiny of his every word and deed by both journalists and the public at large...". It is felt that similar reasoning may be applied to any data subject in public life.

44. Principle 3 does not deal with personal data which, while not being sensitive *stricto sensu*, are nevertheless capable of prejudicing the privacy of data subjects if they are made generally accessible. For example, data held by public bodies concerning human factors such as guardianship, adoption or divorce, etc in civil status registers or registers on births, marriages and deaths may be the cause of distress to individuals if they are made generally accessible. It is felt that member states should elaborate specific policies for the communication of such data based on the need to avoid prejudice being caused to the privacy of data subjects. For example, consideration could be given to communicating such data only to third parties having a legitimate interest in obtaining them, or to preventing or restricting mass delivery of the files in which the data are held.

It is of course the case that names contained in files accessible to third parties may suggest sensitive data, such as racial origin or religion. This point is not treated in the recommendation. It is felt that it is an unavoidable consequence of having one's name included in a public file. Nevertheless, reference should be made to the provisions of Principles 5.2 and 5.7 which seek to regulate the circumstances in which names may be extracted from files accessible to third parties.

4. Generally accessible data

45. Principle 4 provides specific guidance on how "generally accessible data" should be collected by public bodies. Principle 4, it will be seen, is linked to the provisions of Principle 6 since the circumstances surrounding the collection of data will influence the conditions under which they may subsequently be communicated to third parties.

46. Principles 4.1 and 4.2 must be regarded as basic principles of transparency at the stage of data collection. In addition, they reflect the need to ensure that the individual is not to be regarded simply as a rich and unconscious source of personal data. The individual must be brought into the information circuit. Moreover, Principle 4.1 emphasises that the fact that files are to be made accessible to third parties is not a neutral data protection issue. Once again, the need for a legal framework to govern the communication of personal data to third parties is being stressed.

47. All of these safeguards and guarantees contribute to the elaboration of a data protection policy for personal data or personal data files accessible to third parties. As with other principles in the recommendation, they are intended to ensure that the new information market which is being established and which is specifically encouraged in the Guidelines adopted by the Commission of the European Communities referred to earlier does not ignore the fact that personal information is not to be seen simply in terms of an economic commodity. It must also be seen in terms of human rights and fundamental freedoms, in particular the right to data protection.

48. With these factors in mind, Principle 4.1 requires that the purposes for which the data will be collected and processed in files accessible to third parties as well as the public interest justifying their being made accessible should be indicated in accordance with domestic law and practice. The factors mentioned in Principle 4.1 may be indicated either expressly or implicitly, and not necessarily by law. The reference to "practice" allows member states to use means such as the media, official forms or other appropriate mechanisms to indicate the purposes for which data will be collected and processed in files accessible to third parties as well as the public interest motivating their accessibility. For example, it is sufficient that there exists a law on access to public sector information or freedom of information in a particular country which authorises general access to personal data held by public bodies. Moreover, the public interest justifying the accessibility is to be found in the nature of such general legislation - the need to promote an open and accountable public administration. As regards those categories of "public files" in the classic sense of the term, specific statutes very often govern the purposes for which they may be brought into being as well as the reasons why this is the case.

49. As with Principle 4.1, Principle 4.2 refers to domestic law and practice as the appropriate vehicle for communicating to data subjects before or at the time of the collection whether or not they are legally obliged to provide their data to a public body. What may constitute domestic law and practice has been discussed in paragraph 48. In the case of the census or the electoral register, the individual should be informed that he is obliged under law to provide certain personal details. Alternatively, in the case of a telephone directory, the data subject should be informed that there is no legal compulsion to have his data stored in a file which is accessible to third parties. Moreover, data subjects should be informed of the legal basis for data collection as well as the purposes for which the data are to be collected and processed. Finally, data subjects should be informed of the public interest which justifies their data being made accessible to third parties.

50. Principle 4.3 encourages public bodies to be sensitive to the needs of those data subjects whose security and privacy may be particularly at risk if their data were to be made accessible to the public at large. For example, public bodies should heed the requests of individuals working in the security services or who have other legitimate reasons for avoiding publicity not to have their data open to public scrutiny.

5. Access to and communication of personal data by electronic means

51. Principle 5 of the recommendation advances a number of safeguards and guarantees in respect of the personal data which are automatically processed and which are contained in files accessible to third parties. In the first place, the processing operations effected by public bodies are subject to the provisions of domestic law. Such provisions, and they may take the form of specific regulations for various types of electronic databases held by public bodies, should determine how personal data may be communicated to and accessed by third parties. In particular, the use of technical means for communicating or for consulting electronic files should be placed within a legal framework. There are practical ways of doing this. For example, whenever public bodies

make their electronic files available on-line to the public, they should enter into a contract with third parties who wish to download telematically personal data files on to their databases. Such a contract could contain clauses which reflect any conditions and limitations governing the personal data files being sought. In addition, the contract could oblige the third party to respect any conditions which have been imposed by the data subject on subsequent reuse of the data. Moreover, the contract could be used as a vehicle to alert the third party to the need to use personal data in accordance with domestic law and procedure on data protection.

52. The provisions of Principle 5.2 are intended to address the issue of security of the electronic files which may be accessed or consulted on line. Technical measures should be taken so as to prevent mass downloading of personal data files in breach of the regulations governing the keeping and communication of electronic files. In addition, consideration should be given to the possible need to limit the criteria on the basis of which personal data may be searched. This issue is discussed later in the commentary on Principle 6.3.

6. Processing by third parties of personal data originating in files accessible to third parties

53. i. Situation in which the data subject was legally obliged to provide the data (Principle 6.1)

It should be stressed that the term "legally obliged" refers not simply to cases of statutory obligation to provide data, for example in accordance with tax or census obligations, but also covers situations in which data subjects have to provide data in order to receive various social goods or services, for example, education, social security or even the benediction of the state to get married.

ii. Situation in which the data subject volunteered his data to the public body (Principle 6.2)

The data subject may, for example, have replied to a questionnaire sent out by a local authority, answers to which will help the local authority to have an idea of the needs of the local population.

54. Given that the data subject did not have the possibility to opt out of the collection and subsequent inclusion of his data in files accessible to third parties, because he was legally obliged to furnish the data, Principles 6.1 and 6.2 give the data subject compensatory guarantees so as to regulate subsequent processing of his data by third parties. With this in mind, Principle 6.1 requires that the expressed and informed consent of the data subject, and this consent is revocable at any moment, should be sought before the data may be reused by third parties. In order to make the principle of expressed and informed consent meaningful, the individual should of course be asked at the stage of collection whether or not he is willing to allow his personal data to be communicated to third parties by the public body responsible for collecting and making the data accessible. In the

absence of the expressed and informed consent of the data subject, the processing of personal data by third parties must only be carried out in conformity with the requirements laid down in legislative enactments. Such statutory requirements or prescriptions may be included in the laws governing specific categories of public files, data protection legislation or freedom of information legislation.

55. Where the individual has not been obliged to provide his data in the sense described above, he should be able to exercise a number of rights in regard to the data which are stored in a file accessible to third parties. The rights set out in Principle 6.2, paragraphs *a, b, c,* and *d,* need not all be reflected in domestic law. Principle 6.2 makes it clear that they are options, one at least of which should be contained in domestic law.

56. Principle 6.3 emphasises the data protection rights of the data subject in regard to his data which are being processed by third parties and which were obtained from files accessible to third parties. These rights include the right of access, rectification and erasure where the data have been processed contrary to data protection principles. The rights set out in Principle 6.3 are a simple statement of the content of Article 8 of the Data Protection Convention. However, Principle 6.3, second subparagraph, refers in particular to the right of the data subject to have his data erased from those new files which have been brought into existence by third parties on the basis of data accessible to third parties. Although the right to erasure under Article 8 of the Data Protection Convention is conditional on the data having been wrongfully processed, the drafters of the recommendation have felt nevertheless that an unrestricted right to have them disappear is appropriate in the situations covered by this recommendation. It may be noted that the approach of the drafters to the right to erasure is compatible with an earlier approach followed in Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing. Reference should be made to this recommendation for additional principles governing the way in which personal data covered by the present recommendation may be reused by third parties for marketing purposes.

7. File interconnection/matching

57. The principles contained in this recommendation are intended to be technologically relevant. As noted in various parts of the text, the main concerns are directed at avoiding possible abuses arising out of the introduction and use of data processing technology by public bodies and the new electronic means of communicating the data which they hold.

58. Data processing technology is also at the disposal of third parties to whom the data may be communicated. Using software techniques, they may scan public files electronically with a view to isolating names and addresses on the basis of certain criteria - for example age or racial origin. Third parties are now able to produce new and more interesting data files out of information contained in various unrelated files held by public bodies. The new files which come into existence as a result of this process may be extremely rich in terms of personal data, and certainly more informative than one file taken by itself. For example, it is possible to interconnect an electronic telephone

directory with another category of public file so as to enhance the value of the information contained in the electronic telephone directory.

59. There are obvious dangers in these techniques of file interconnection or file matching. In particular they may produce automatic lifestyle profiles on individuals without their knowledge and consent. In addition, the possibility to isolate names from public files on the basis of the nationality or religion suggested by the name allows files to be created containing sensitive data. It is for this reason that Principle 5.2 of the recommendation has proposed limitations on the scope of electronic interrogations or electronic searches of files accessible to the public. For example, consideration should be given to the need to prevent electronic searches of public files which are limited to particular names of people living in specific regions or localities. The downloading of such information, coupled with the possibility of matching or interconnecting it with another file, could allow third parties to have quite precise data of a sensitive nature on well-defined groups.

60. Aware of the problems discussed in the previous paragraph, the drafters of the recommendation have recommended that file matching or file interconnection techniques should only be permissible if domestic law permits them. In addition, domestic law - which once again should be interpreted broadly - should provide appropriate safeguards for the data subject in the event of authorisation being given to third parties to use these techniques.

8. Transborder data flows

61. The principles discussed so far address specific national contexts in which personal data or personal data files are communicated by public bodies to third parties. The safeguards and guarantees discussed up to now are based on considerations of domestic law. However, the communication of personal data or personal data files held by public bodies in one country to third parties situated in other countries cannot be ignored. The state of technology now enables third parties to access remotely, from country A, personal data files held by public bodies in country B. The data may, for example, be downloaded from one country to another country. Alternatively, magnetic tapes may be sent by public bodies through the postal service to third parties resident in another state. In other words, it is also necessary to discuss the data protection issues raised in this sector in the context of transborder communication of personal data or personal data files (Principle 8.1).

62. The drafters of the recommendation have sought to adapt the principles of Article 12 of the Data Protection Convention so as to provide specific principles for communication in this sector. Principle 8 of the recommendation analyses a number of situations in which transborder communication may take place:

- the communication may be to the territory of a state which has ratified the convention;

- the communication may be to the territory of a state which, although not a Contracting Party to the convention, nevertheless has legal provisions in conformity with the convention and with the present recommendation;
- the communication may be to the territory of a state which is not possessed of legal provisions in conformity with the convention or with this recommendation.

63. Taking in turn each of the various hypotheses outlined above, the drafters of the recommendation have provided the following legal framework for transborder data flows.

64. As regards the first hypothesis and in accordance with the principles of Article 12, paragraph 2, of Convention No. 108, Principle 8.2 of the recommendation sets out the principle of the free flow of data. Since a Contracting Party to the convention must be possessed of data protection norms consistent with the treaty's basic principles, there is no *prima facie* justification for restricting the flow of data to it. This is certainly the case when the exporting state is also a Contracting Party.

However, Principle 8 of the recommendation is not exclusively concerned with the situation in which the communicating country is a Contracting Party. It also envisages personal data being communicated by non-Contracting Parties, including states which have not yet adopted legislation on data protection. The drafters of the recommendation have sought to encourage the acceptance by all countries of the principle of the free flow of data to states which have ratified Convention No. 108.

The provisions of Principle 8.2 are without prejudice to the right of a Contracting Party to determine the conditions for the transfer of particular categories of personal data or personal data files in accordance with the provisions of Article 12, paragraph 3.*a*, of Convention No. 108.

65. Principle 8.3 deals with the situation in which the receiving state has legal provisions which reflect the basic principles of Convention No. 108 as well as the philosophy of this recommendation, but has not yet ratified the convention. Certain states have in fact adopted data protection laws in conformity with the convention but have not yet reached the stage of depositing their instruments of ratification. As with Principle 8.2. Principle 8.3 similarly encourages the free flow of data to such states. It is felt that, even though ratification of the convention is an absolute necessity at some stage, the legal situation in regard to data protection in such countries should be accepted as sufficient and transfrontier communication should be allowed to take place without further conditions. To use the terminology of the convention, an "equivalent level of protection" may be deemed to exist in such countries, at least when the data are to be exported from the territory of Contracting Parties.

66. Principle 8.4 deals with a situation in which the country of destination has not ratified Convention No. 108 and possesses no legal provisions on the protection of personal data or at least no provisions which may be considered as being compatible with the basic principles of the convention. In this case, and so as not to weaken the protection of data subjects and thus undermine the scope of data protection principles, in particular the

principles laid down in the convention as well as this recommendation, exporting states should consider imposing restrictions on the communication of personal data to third parties resident in such countries.

67. In the first place, the drafters of the recommendation have suggested that no communication should take place in the absence of the free and informed consent in writing of the data subject. In addition, such consent should be revocable at any time. It is thought that increasing the level of the consent requirement so as to include "written consent" is justified in the circumstances envisaged in Principle 8.4, since the individual's data are to be communicated outside his national territory to a country where it is impossible to monitor the fate of the data.

68. Principle 8.4 also provides for an alternative method of ensuring data protection in the event of communication of data to countries which have not yet legislated for data protection. The alternative method envisages the exporting country adopting measures which could guarantee the integrity of the data, including respect for the principles laid down in the convention and in this recommendation, in the territory of the country of destination. One such measure could require the importing third party to commit himself contractually to respecting data protection principles. In this regard, reference should be made to the draft model contract which has been drawn up by the Consultative Committee of the Contracting Parties to Convention No. 108. The use of contract law, it should be emphasised, is to be regarded as a stopgap measure pending the enactment of data protection provisions in the country of destination and should not be seen as replacing the need to adopt such provisions at some stage. So as to allow for dispute resolution free from considerations of national law, the contract should provide for a system of independent arbitration. The competence of the independent arbitrators should extend to enabling the data subject to enforce his rights in regard to his data and to awarding him compensation in the event of such rights being denied by the third party. Principle 8.4 stresses that the use of such measures as an alternative to requiring the free, informed and written consent of the data subject is conditional on the data subject being informed of the possibility that his data may be communicated to third parties situated in countries not having data protection provisions, and on being given the opportunity to object to the communication.

69. Principle 8.5 highlights a particular problem raised by the transborder possibilities of on-line access to or remote downloading of generally accessible data or data files. This problem is rendered more acute in the case of communication to states without data protection legislation. Given the concern of the drafters of the recommendation to produce a text which is technologically relevant, it was felt important to bring the issue of remote consultation or downloading from abroad to the attention of national legislators.

9. Co-ordination/co-operation

70. Reference was made in the operative part of the preamble to the recommendation of the need to bring it "to the attention of authorities set up under data protection legislation or legislation on access to public sector information". Principle 9 of the recommendation

encourages a cross-fertilisation of the role of such authorities so as to ensure consistency of approach to the communication to third parties of personal data or personal data files held by public bodies. The dialogue encouraged in Principle 9 should allow the respective agencies to have information on the conditions which should govern communication. By way of illustration: the communication of personal data under provisions governing freedom of information is invariably restricted where communication would result in prejudice being caused to the privacy of the data subject. The interpretation of such a proviso is usually left undefined in freedom of information legislation. It is felt that authorities entrusted with the interpretation of the proviso could usefully borrow from the conditions which have been laid down by data protection authorities on the use which may be made of personal data which have been declared or notified or registered with them. Given that data protection authorities may place limitations on the use which may be made by public bodies, including communication, of the personal data files which they hold, it is felt appropriate that the agency operating under freedom of information legislation should take note of those conditions.