

**Recommendation No.R (87) 15 of the Committee of Ministers to Member States
regulating the use of personal data in the police sector**

*(Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of
the Ministers' Deputies)*

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council
of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between
its members;

Aware of the increasing use of automatically processed personal data in the police sector
and of the possible benefits obtained through the use of computers and other technical
means in this field;

Taking account also of concern about the possible threat to the privacy of the individual
arising through the misuse of automated processing methods;

Recognising the need to balance the interests of society in the prevention and suppression
of criminal offences and the maintenance of public order on the one hand and the
interests of the individual and his right to privacy on the other;

Bearing in mind the provisions of the Convention for the Protection of Individuals with
regard to Automatic Processing of Personal Data of 28 January 1981 and in particular the
derogations permitted under Article 9;

Aware also of the provisions of Article 8 of the Convention for the Protection of Human
Rights and Fundamental Freedoms,

Recommends the governments of member states to:

- be guided in their domestic law and practice by the principles appended to this
Recommendation, and
- ensure publicity for the provisions appended to this Recommendation and in particular
for the rights which its application confers on individuals.

Appendix to Recommendation No. R (87) 15

Scope and definitions

The principles contained in this Recommendation apply to the collection, storage, use and
communication of personal data for police purposes which are the subject of automatic
processing.

For the purposes of this Recommendation, the expression "personal data" covers any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time, cost and manpower.

The expression "for police purposes" covers all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order.

The expression "responsible body" (controller of the file) denotes the authority, service or any other public body which is competent according to national law to decide on the purpose of an automated file, the categories of personal data which must be stored and the operations which are to be applied to them.

A member state may extend the principles contained in this Recommendation to personal data not undergoing automatic processing.

Manual processing of data should not take place if the aim is to avoid the provisions of this Recommendation.

A member state may extend the principles contained in this Recommendation to data relating to groups of persons, associations, foundations, companies, corporations or any other body consisting directly or indirectly of individuals, whether or not such bodies possess legal personality.

The provisions of this Recommendation should not be interpreted as limiting or otherwise affecting the possibility for a member state to extend, where appropriate, certain of these principles to the collection, storage and use of personal data for purposes of state security.

Basic principles

Principle 1 - Control and notification

1.1. Each member state should have an independent supervisory authority outside the police sector which should be responsible for ensuring respect for the principles contained in this Recommendation.

1.2. New technical means for data processing may only be introduced if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation.

1.3. The responsible body should consult the supervisory authority in advance in any case where the introduction of automatic processing methods raises questions about the application of this Recommendation.

1.4. Permanent automated files should be notified to the supervisory authority. The notification should specify the nature of each file declared, the body responsible for its processing, its purposes, the type of data contained in the file and the persons to whom the data are communicated.

Ad hoc files which have been set up at the time of particular inquiries should also be notified to the supervisory authority either in accordance with the conditions settled with the latter, taking account of the specific nature of these files, or in accordance with national legislation.

Principle 2 - Collection of data

2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

2.2. Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.

2.3. The collection of data by technical surveillance or other automated means should be provided for in specific provisions.

2.4. The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry.

Principle 3 - Storage of data

3.1. As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law.

3.2. As far as possible, the different categories of data stored should be distinguished in accordance with their degree of accuracy or reliability and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments.

3.3. Where data which have been collected for administrative purposes are to be stored permanently, they should be stored in a separate file. In any case, measures should be taken so that administrative data are not subject to rules applicable to police data.

Principle 4 - Use of data by the police

4. Subject to Principle 5, personal data collected and stored by the police for police purposes should be used exclusively for those purposes.

Principle 5 - Communication of data

5.1. Communication within the police sector

The communication of data between police bodies to be used for police purposes should only be permissible if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

5.2.i. Communication to other public bodies

Communication of data to other public bodies should only be permissible if, in a particular case:

- a. there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority, or if
- b. these data are indispensable to the recipient to enable him to fulfil his own lawful task and provided that the aim of the collection or processing to be carried out by the recipient is not incompatible with the original processing, and the legal obligations of the communicating body are not contrary to this.

5.2.ii. Furthermore, communication to other public bodies is exceptionally permissible if, in a particular case:

- a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if
- b. the communication is necessary so as to prevent a serious and imminent danger.

5.3.i. Communication to private parties

The communication of data to private parties should only be permissible if, in a particular case, there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority.

5.3.ii. Communication to private parties is exceptionally permissible if, in a particular case:

- a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if
- b. the communication is necessary so as to prevent a serious and imminent danger.

5.4. International communication

Communication of data to foreign authorities should be restricted to police bodies. It should only be permissible:

- a. if there exists a clear legal provision under national or international law,
- b. in the absence of such a provision, if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law,

and provided that domestic regulations for the protection of the person are not prejudiced.

5.5.i. Requests for communication

Subject to specific provisions contained in national legislation or in international agreements, requests for communication of data should provide indications as to the body or person requesting them as well as the reason for the request and its objective.

5.5.ii. Conditions for communication

As far as possible, the quality of data should be verified at the latest at the time of their communication. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated and data based on opinions or personal assessments checked at source before being communicated and their degree of accuracy or reliability indicated.

If it is discovered that the data are no longer accurate and up to date, they should not be communicated. If data which are no longer accurate or up to date have been communicated, the communicating body should inform as far as possible all the recipients of the data of their nonconformity.

5.5.iii. Safeguards for communication

The data communicated to other public bodies, private parties and foreign authorities should not be used for purposes other than those specified in the request for communication.

Use of the data for other purposes should, without prejudice to paragraphs 5.2 to 5.4 of this principle, be made subject to the agreement of the communicating body.

5.6. Interconnection of files and on-line access to files

The interconnection of files with files held for different purposes is subject to either of the following conditions:

- a. the grant of an authorisation by the supervisory body for the purposes of an inquiry into a particular offence, or
- b. in compliance with a clear legal provision.

Direct access/on-line access to a file should only be allowed if it is in accordance with domestic legislation which should take account of Principles 3 to 6 of this Recommendation.

Principle 6 - Publicity, right of access to police files, right of rectification and right of appeal

6.1. The supervisory authority should take measures so as to satisfy itself that the public is informed of the existence of files which are the subject of notification as well as of its rights in regard to these files. Implementation of this principle should take account of the specific nature of ad hoc files, in particular the need to avoid serious prejudice to the performance of a legal task of the police bodies.

6.2. The data subject should be able to obtain access to a police file at reasonable intervals and without excessive delay in accordance with the arrangements provided for by domestic law.

6.3. The data subject should be able to obtain, where appropriate, rectification of his data which are contained in a file.

Personal data which the exercise of the right of access reveals to be inaccurate or which are found to be excessive, inaccurate or irrelevant in application of any of the other principles contained in this Recommendation should be erased or corrected or else be the subject of a corrective statement added to the file.

Such erasure or corrective measures should extend as far as possible to all documents accompanying the police file and, if not done immediately, should be carried out, at the latest, at the time of subsequent processing of the data or of their next communication.

6.4. Exercise of the rights of access, rectification and erasure should only be restricted insofar as a restriction is indispensable for the performance of a legal task of the police or is necessary for the protection of the data subject or the rights and freedoms of others.

In the interests of the data subject, a written statement can be excluded by law for specific cases.

6.5. A refusal or a restriction of those rights should be reasoned in writing. It should only be possible to refuse to communicate the reasons insofar as this is indispensable for the performance of a legal task of the police or is necessary for the protection of the rights and freedoms of others.

6.6. Where access is refused, the data subject should be able to appeal to the supervisory authority or to another independent body which shall satisfy itself that the refusal is well founded.

Principle 7 - Length of storage and updating of data

7.1. Measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored.

For this purpose, consideration shall in particular be given to the following criteria: the need to retain data in the light of the conclusion of an inquiry into a particular case; a final judicial decision, in particular an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject; particular categories of data.

7.2. Rules aimed at fixing storage periods for the different categories of personal data as well as regular checks on their quality should be established in agreement with the supervisory authority or in accordance with domestic law.

Principle 8 - Data security

8. The responsible body should take all the necessary measures to ensure the appropriate physical and logical security of the data and prevent unauthorised access, communication or alteration.

The different characteristics and contents of files should, for this purpose, be taken into account.

Explanatory Memorandum

Introduction

1. Although the data protection principles laid down in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known also as the Data Protection Convention), of 28 January 1981, are of general application to the collection, storage, use, etc of personal data in both the private and public sectors, it has been felt necessary to adapt them to the specific requirements of particular sectors.

2. This "sectoral approach" to data protection has so far led to the adoption by the Committee of Ministers of the Council of Europe of four recommendations elaborated by its intergovernmental Committee of experts on data protection (CJ-PD): Recommendation No. R (81) 1 on regulations for automated medical data banks (23 January 1981), Recommendation No. R (83)10 on the protection of personal data used for scientific research and statistics (23 September 1983), Recommendation No. R (85) 20 on the protection of personal data used for purposes of direct marketing (25 October 1985), and Recommendation No. R (86) 1 on the protection of personal data used for social security purposes (23 January 1986).

3. Within the framework of this sectoral approach, the Committee of experts on data protection believed it was appropriate to reflect on the data protection problems created by the use of personal data in the police sector with a view to preparing a legal instrument setting out a number of principles designed to regulate the collection, storage, use, communication and conservation of personal data by the police and which would be inspired by the norms laid down in the Data Protection Convention.

4. Given the increased activities of police forces in the lives of individuals necessitated by new threats to society posed by terrorism, drug delinquency, etc as well as a general increase in criminality, it was felt even more necessary to establish clear guidelines for the police sector which indicate the necessary balance needed in our societies between the rights of the individual and legitimate police activities when the latter have recourse to data-processing techniques.

5. Bearing in mind that Article 9, paragraph 2, of the Convention makes it possible for member states to derogate from the Convention's basic data protection principles in the interests of, inter alia, "the suppression of criminal offences", the committee of experts mandated a working party to identify the sort of problems raised by the use of personal data in the police sector and to formulate concrete proposals for their solution. The working party was composed of experts from Belgium, France, Italy, the Netherlands, Portugal, Sweden, Switzerland and the United Kingdom. Under the chairmanship of Dr R. Schweizer (Switzerland), the working party met on five occasions.

6. In the course of the first meeting (19 and 20 December 1983), the working party attempted to identify the extent to which the legislation of the member states contained specific provisions regulating the use of personal data in the police sector. In addition, it gained a broad view of the sort of problems which this sector poses for data protection. In this regard, the task of the working party was facilitated by a study prepared by a consultant, Professor H. Maisl (France).

7. At its second meeting (18 to 20 June 1984), the members of the working party explored the issues further, taking account of the replies which were submitted by the member states in response to a questionnaire. In addition, the working party analysed the relevant case-law of the European Court and European Commission of Human Rights in the context of Article 8 of the European Convention on Human Rights, which has a bearing on the collection, use, storage, etc of personal data by the police. A preliminary

draft instrument emerged from the discussions which reflected the working party's provisional views on ways of regulating the use of personal data in the police sector.

8. At its third meeting (17 to 19 December 1984), the working party proceeded to revise the preliminary draft instrument. Careful consideration was given in particular to the scope of the derogation set out in Article 9, paragraph 2, of the Data Protection Convention. The working party proceeded on the basis that it would be appropriate to establish a special set of data protection principles for the classic and crucial tasks of the police while at the same time adapting them to take account of particular requirements, notably in respect of the "suppression of criminal offences".

9. Building on the comments and observations submitted by the plenary committee which was kept informed of the working party's progress, the working party expanded its analysis in its subsequent meetings (5 to 7 June 1985; 27 to 29 November 1985) so as to deal with such issues as the communicating of data by the police to third parties, in particular transborder data flows. The finalised text was submitted to the plenary committee along with a draft explanatory memorandum prepared by the Secretariat.

10. The committee of experts approved the draft recommendation and draft explanatory memorandum at its 13th meeting (4 to 7 November 1986) after detailed examination and decided to submit these texts to the European Committee on Legal Co-operation (CDCJ) for examination and approval.

11. The draft recommendation and draft explanatory memorandum were approved by the European Committee on Legal Co-operation on 22 May 1987.

12. Recommendation No. R (87) 15, regulating the use of personal data in the police sector, was adopted by the Committee of Ministers of the Council of Europe on 17 September 1987.

Detailed comments

Preamble

13. Technology inevitably facilitates the work of the police. In a sector where the collection and storage of a vast amount of personal information are indispensable in view of the wide-ranging and important role of police forces in society, the advantages to be gained from the use of technology are apparent. Sophisticated criminality inevitably requires access to countervailing sophisticated methods of law enforcement. Computers, in particular, have allowed the police to enhance its efficiency in the collection and storage of personal data and have contributed to more rapid decision-making in law enforcement for the benefit of society.

14. However, the concerns which prompted the elaboration of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 in regard to the increasing recourse to automation in all sectors are most

acutely felt in the police sector. For it is in this domain that the consequences of a violation of the basic principles laid down in the Convention could weigh most heavily on the individual.

15. The preamble recognises the need to strike a balance between the interests involved - the interests of the individual and his right to privacy and the interests of society in the prevention and suppression of criminal offences and the maintenance of public order.

16. Not surprisingly, the balance is difficult to achieve in the police sector. Both Article 8, paragraph 2, of the European Convention on Human Rights and Article 9 of the Data Protection Convention allow for exceptions to be made to the rights which they offer.

17. Although the preamble refers to the possible threat to the privacy of the individual through the misuse of automated processing methods, it should be borne in mind that privacy is not to be interpreted simply in terms of protection of one's private sphere against intrusive conduct. It is for this reason that the preamble draws attention to Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, and the legality of certain technical surveillance means to obtain data on individuals must be tested against the provisions of Article 8 and the relevant rulings of the European Court of Human Rights.

18. Recourse to wire-tapping and interception of mail are examples of abuse of one's private life *stricto sensu*. The European Court of Human Rights has so ruled on two occasions (Case of Klass and others, judgment of 6 September 1978, Series A, No. 28; Malone Case, judgment of 2 August 1984, Series A, No. 82). Principles 2.2 and 2.3, in particular, must be interpreted in the light of the Court's case-law.

19. However, the preamble also refers to the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, of 28 January 1981, which goes beyond traditional privacy notions and sets out a series of basic protective principles designed to regulate the collection, storage, use and communication of personal data.

20. Specific reference is made in the preamble to the derogations permitted under Article 9 of the Data Protection Convention and it will be recalled that a derogation from the provisions of Article 5 ("quality of data"), Article 6 (rules for "specific categories of data") and Article 8 ("additional safeguards for the data subject") is authorised only if it is provided for by law and constitutes a necessary measure in a democratic society in the interests of, *inter alia*, the "suppression of criminal offences". Bearing in mind that the European Court of Human Rights in its judgment in the Malone Case laid down a number of strict criteria (precision, certainty, foreseeability, etc), it is thought that the principles contained in this non-binding legal instrument can provide helpful guidance to the legislator as to the interpretation of the derogation in Article 9, paragraph 2, of the Data Protection Convention when regulating the collection, use, etc of personal data in the

police sector. This point should be borne in mind, for example, in the context of paragraph 2.1.

21. As so worded, the scope of the derogation is narrower than the societal interests outlined in the fifth paragraph of the preamble. However, the aim of the present Recommendation is to establish a special set of data protection principles for the classic and crucial tasks of the police while at the same time adapting the principles to take account of particular requirements, notably in respect of the "suppression of criminal offences". It goes without saying that personal data collected and used for tasks not falling within classic police activities, for example for administrative purposes, are subject to general data protection norms.

Scope and definitions

22. The principles are intended to regulate all the crucial stages where data protection becomes an issue - collection, storage, use and communication of personal data. It will be noted that these activities are linked to the finality of "police purposes". The latter term is defined in the light of the interests at stake for society, already referred to in the fifth paragraph of the preamble. However, it will be recalled that this statement of finality will be the subject of refinement at later stages in the text so as to ensure that the principles will treat differently the tasks which the police must perform in regard to the suppression of criminal offences and the tasks which it must carry out at the level of prevention and the maintenance of public order.

23. The Recommendation refers simply to "police authorities". It should be borne in mind that, depending on the legal system in question, different police forces can coexist. It may not always be easy to distinguish between them from the point of view of division of labour. However, regardless of nomenclature, the principles should apply to any body with police functions involved in the collection, storage, use and transfer of personal data for the purposes set out in the third paragraph of this section.

24. The Recommendation is primarily concerned with automated personal data, and the term "personal data" is defined so as to be consistent with its use in earlier recommendations of the Council of Europe in the field of data protection. It is worth repeating that whether or not an individual is to be regarded as "identifiable" is to be determined objectively, bearing in mind the sophistication of methods of identification at the disposal of the police, for example fingerprint techniques, voice recognition systems, data base surveillance, etc.

25. The "responsible body" referred to in this section is in reality, to use the terminology of the Convention, the controller of the file. Accordingly, this body will have ultimate responsibility for the file. It will be seen in Principle 1.4 that the name of the responsible body for a particular file should be notified to the supervisory body.

26. Although the instrument confines itself to automated personal data - as is the case for the laws of a certain number of member states, - it is recognised that certain member

states of the Council of Europe still rely heavily on manual files. In addition, in other countries where police computerisation is highly advanced the data stored on computers may sometimes only be intelligible if reference is made to manual files. It would be undesirable, therefore, to exempt manual files and it is for this reason that the instrument accepts that member states have the freedom to extend the principles to data held in manual form. Paragraph 38, it will be seen, provides guidance on how member states can treat the issue of manually held data.

27. With the passage of time, of course, more and more data which are presently held in manual form will be automated and the principles contained in this instrument will extend to them. It should not be permissible, however, for a member state to deliberately circumvent the guarantees laid down in this instrument by transferring personal data from automated files to manual files. It is recognised, however, that it may be difficult to determine whether there has been a deliberate circumvention when data are deleted pursuant to Principle 7 but a print-out of the data has been retained.

28. In accordance with Article 3, paragraph 2, of the Data Protection Convention, the instrument also accepts that member states have the possibility of applying the principles to legal persons.

29. Finally, with regard to matters of state security, which the explanatory report to the Data Protection Convention describes as "protecting national sovereignty against internal or external threats, including the protection of the international relations of the state", it would seem desirable to recognise the freedom of member states to extend some of the safeguards which are set out in this instrument to the field of state security wherever their application seems feasible and relevant.

30. Over and above the particular contexts of state security and legal persons, it should be remembered that the principles outlined in the Recommendation were considered by the drafters as minimum guarantees and that member states retain the liberty of course to lay down stronger measures of protection.

Principle 1 - Control and notification

31. Data protection authorities or commissioners play a central role in the framework of domestic data protection laws. Where such bodies exist, they should be entrusted with the tasks set out in this Recommendation. It would be undesirable to create a competing, separate organ for the purposes of the Recommendation. However, any new organ created should be genuinely independent of police control, a crucial quality given that the Recommendation at certain stages provides for the possibility of conferring decision-making powers on it involving the evaluation of the limits of police action with regard to the use of personal data.

32. The constitutional structure of certain member states may necessitate the creation of several independent supervisory authorities where data protection authorities or commissioners do not already exist. The body need not necessarily be a collegiate one. It

would be possible for an individual to discharge the role of "ensuring respect for the principles contained in this Recommendation". However, given the importance of this role, it is desirable that the supervisory authority, regardless of the form which it takes, should have sufficient resources to enable it to be effective.

33. Finally, it should be stressed that the absence of general data protection legislation does not constitute a bar to the creation of an independent supervisory authority for the police sector. The principles set out in this Recommendation are addressed to all member states and can be taken up by countries which have yet to adopt general norms for data protection.

34. The preamble recognises that, in addition to computers, new technical means for data processing present advantages for police work, for example voice-recognition systems, machine-readable identification cards, computer-based surveillance techniques, electronic tracking systems. However, given their possible misuse, it is essential that their introduction and use are accompanied by awareness of their implications for the individual. It is for this reason that Principle 1.2 recommends that careful consideration be given to their introduction so as to ensure that they will not undermine the spirit of existing data protection legislation. In addition, public debate would seem desirable in regard to the introduction of new technologies which pose possible threats to privacy and which were not in the mind of the legislator at the time of adoption of data protection norms.

35. In this regard, the independent supervisory authority has a useful role to perform. In accordance with Principle 1.3, it should be empowered to make observations, at the request of the responsible body, when the latter intends to introduce automatic data-processing methods which may possibly pose problems for the application of the Recommendation. Principle 1.3 does not imply a right of veto on the introduction of such methods. However, it allows the supervisory authority to examine the proposed methods to see whether they will, for example, escape the guidelines concerning the communication of data (Principle 5). It could advise the responsible body on the sort of measures to be taken so as to ensure respect for the Recommendation's principles.

36. For the purpose of this instrument, police files cover all structured/ organised personal data which are managed by the police services to meet their requirements in regard to the prevention or suppression of criminal offences or the maintenance of public order. Police files as so defined enable the police to retrieve information relating to identified or identifiable persons. Principle 1.4 obliges the police, or perhaps some other body designated by national law, to notify its automated files to the supervisory authority and to specify certain details concerning each automated file.

37. It will be noted that this is a general requirement of notification. No exception is laid down in favour of files appertaining solely to the suppression of criminal offences. As stated previously, the Recommendation attempts to lay down particular rules for the classic tasks of the police, only departing from them where it is found necessary to take

account of the particular requirements of the police in the context of the "suppression of criminal offences".

38. Although the rule on notification is restricted to automated police files, it may be the case that certain member states will avail of their right to extend the principles laid down in this instrument to manual police files. Should this be the case, a member state may oblige the police to keep a description of each type of manual file kept, the controller of the file, its purpose, the sort of data contained in it and the persons to whom the data are communicated. Such general descriptions would be notified to the supervisory authority. Alternatively, the need to notify every description could be obviated if each police force were required to ensure that its manual files conformed to a certain description drawn up at central level. If a police force did not comply with this general description, it could be obliged to make its own description and to notify it to the supervisory authority.

39. Other ways of extending the principles to manual files are, of course, possible.

40. The second sub-paragraph of Principle 1.4 addresses the issue of ad hoc files which have been set up at the time of particular inquiries.

Notification of every ad hoc file could create unacceptable bureaucracy. However, such files should not escape some sort of notification. National law may lay down the circumstances in which they are to be brought to the attention of the supervisory authority. It may be that domestic law will only require notification of the existence of such files or a global notification of ad hoc files of a particular type, allowing the supervisory authority to inquire into them so as to ensure that they conform to the principles of data protection.

41. Alternatively, in the absence of guidance from national law, the supervisory authority, in collaboration with the responsible body referred to previously, could work out guidelines governing the notification of ad hoc files. For example, it may emerge from the dialogue between the supervisory authority and the responsible body that such files should be notified after they have been in existence for a reasonable time, or if it can be presumed that they will be in existence for a reasonable time. Other criteria for notification will be found.

42. Files brought into existence for the purposes of a particular inquiry which is quickly cleared up should not need to be notified.

Principle 2 - Collection of data

43. Principle 2.1 excludes an open-ended, indiscriminate collection of data by the police. It expresses a qualitative and quantitative approach to Article 5.c of the Data Protection Convention which stipulates that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are stored. Given that Article 9.a of the convention allows a derogation from this principle in regard to the "suppression of criminal offences", Principle 2.1 of the Recommendation attempts to fix the boundaries

to this exception by limiting the collection of personal data to such as are necessary for the prevention of a real danger or the suppression of a specific criminal offence, unless domestic law clearly authorises wider police powers to gather information. "Real danger" is to be understood as not being restricted to a specific offence or offender but includes any circumstances where there is reasonable suspicion that serious criminal offences have been or might be committed to the exclusion of unsupported speculative possibilities. By way of example, reasonable suspicion that unspecified drugs were being illegally brought into a country through a port by unidentified private yachts would justify the collection of data on all such yachts using that port, but not all yachts, their owners and passengers using every port in that country.

44. Principle 2.2 addresses the issue of the collection and storage of data without the data subject being aware of this and attempts to offer a regulatory principle when it is decided to retain the data so collected, namely the person on whom data have been collected without his knowledge should be informed that data are being held on him as soon as the object of the police activities is no longer likely to be prejudiced. Of course this procedure will be unnecessary if the police has decided to delete the data collected unbeknown to the individual.

It is accepted that Principle 2.2 may prove difficult to implement where street videos and similar mass surveillance methods are an issue and information has been collected on a great number of persons. It is for this reason that the principle recommends informing those subjected to a secret surveillance that data are still held on them only "where practicable". The police themselves will be expected to take the decision.

45. It is thought that member states may find this principle of value when considering the case-law of the European Commission of Human Rights which, in the context of Article 8 of the European Convention on Human Rights, has recognised that the collection and storage of data on an individual without his knowledge could raise an issue of data protection (Application No. 8170/78, X v. Austria, Application No. 9248/81, Leander v. Sweden).

46. While Principle 2.2 places the emphasis on the storage of personal data collected unbeknown to the data subject, whether by secret means or non-secret means (for example, asking questions of the data subject's neighbours), Principle 2.3 focuses on the collection of data by technical surveillance or other automated means. Specific provisions in national law should govern collection of data by such methods. In particular, the case-law of the European Court of Human Rights should be borne in mind when recourse is had to wiretapping. The judgment in the Malone case states that such a form of technical surveillance must be authorised with reasonable precision in accessible legal rules that sufficiently indicate the scope and manner of exercise of the discretion conferred on the authorities and be accompanied by adequate guarantees against abuse.

47. Law-enforcement agencies work within the confines of the law and their data collection activities are thus circumscribed. Accordingly, domestic legal provisions, which must take as their minimum basis the provisions of the Convention for the

Protection of Human Rights and Fundamental Freedoms (1950), must be respected. In this regard, account must also be taken of the case-law of the European Commission and European Court of Human Rights in the areas of arrest or detention for questioning, search and seizure, methods of interrogation, the taking of body samples, fingerprints and photographs, etc. It goes without saying that the relevant domestic legislation must conform to the provisions of the Convention as interpreted by the European Court of Human Rights.

48. Principle 2.4 treats the issue of sensitive data and reflects the concern expressed in Article 6 of the Data Protection Convention that the collection and storage of particular categories of data should be restricted. It may be the case that the collection of certain sensitive data will be necessary for the purposes set out in Principle 2.1. However, in no circumstances should such data be collected simply in order to allow the police to compile a file on certain minority groups whose behaviour or conduct is within the law. The collection of such data should only be authorised if "absolutely necessary for the purposes of a particular inquiry". The expression "a particular inquiry" should be seen as a general limitation; such an inquiry should be based on strong grounds for believing that serious criminal offences have been or may be committed. The collection of sensitive data in such circumstances should, moreover, be "absolutely necessary" for the needs of such inquiries.

The reference to sexual behaviour does not apply where an offence has been committed.

Principle 3 - Storage of data

49. Personal data when collected will subsequently be the subject of a decision concerning their storage in police files. Principle 3.1 addresses the requirements of accuracy and storage limitation. The data stored should be accurate and limited to such data as are necessary to enable the police to perform its lawful tasks. Principle 3.1 recognises that, in addition to national law, international law which for the purposes of this Recommendation is taken to include international co-operation within the framework of Interpol, may also be the source of lawful police work (for example, international legal agreements on co-operation between national police forces) which justifies the storage of data.

50. This principle is important given the fact that the commitment of personal data to a police file may lead to a permanent record and indiscriminate storage of data may prejudice the rights and freedoms of the individual. It is also in the interests of the police that it has only accurate and reliable data at its disposal.

51. It will be noted that Principle 3 as a whole is a general requirement aimed at all types of data collected for police purposes as defined previously.

52. Principle 3.2 encourages the implementation of a system of data classification. It is thought that it should be possible to distinguish between corroborated data and uncorroborated data, including assessments of human behaviour, between facts and

opinions, between reliable information (and the various shades thereof) and conjecture, between reasonable cause to believe that information is accurate and a groundless belief in its accuracy.

53. Data collected and stored by the police for administrative purposes (for example, information on firearms certificates granted, lost property, etc) are of course subject to the general principles of data protection. Principle 3.3 recommends that such data be held separately from data stored for police purposes within the meaning of this instrument when it is decided to retain them indefinitely. It would be wrong in principle to allow the special regime for police data, with its particular approach to data protection in the police sector, to extend to them.

54. However, it may not always be feasible to ensure a strict separation between the two types of data. Nevertheless, in such a case, member states should examine the sort of measures which could be taken in the event of unavoidable mixing so as to ensure that administrative data remain fully subject to the general rules of data protection.

Principle 4 - Use of data by the police

55. Principle 4 states clearly the notion of finality: personal data collected for the prevention and suppression of criminal offences or for the maintenance of public order ("police purposes") must only be used for those purposes. However, the absolute nature of this rule is modified in part by Principle 5.

Principle 5 - Communication of data

56. Principle 5 is structured in such a way as to regulate separately the various forms of data transfer that can legitimately take place while at the same time providing general principles applicable to all the transfers envisaged.

57. Transfer of data within the police sector is made conditional on the receiving police authority possessing a legitimate interest in obtaining the data, for example that the data are needed by the recipient for the prevention or suppression of criminal offences or the maintenance of public order. It is accepted that a police body requesting information from another police body may communicate certain data so that its request for information can be met provided that both parties to the communication fulfil the legitimate interest requirement laid down in Principle 5.1.

58. Outside the framework of communication within the police sector, the conditions governing transfer are stricter, given the fact that the communication may be for non-police purposes *stricto sensu*. The exceptional nature of the circumstances allowing communication set out in Principles 5.2 and 5.3 is stressed. It will be noted that circumstances a and b in both Principles 5.2.ii and 5.3.ii are specifically referred to as "exceptional".

59. The public bodies referred to in Principle 5.2 could, for example, be social security authorities or inland revenue authorities investigating fraud, or immigration control, customs authorities and so on.

60. The general conditions for data transfer to such bodies are set out in Principle 5.2.i, sub-paragraphs a and b. It will be noted that Principle 5.2.i.a envisages the possibility of the supervisory authority authorising a data transfer. It is with this sort of role in mind that emphasis was placed in Principle 1 on the need for the supervisory authority to be independent of the police sector.

The "clear legal authorisation" referred to in Principle 5.2.i.a could be provided by a magistrate.

61. Mutual assistance between police authorities and the sort of public bodies suggested above is also possible in the absence of the circumstances set out in Principle 5.2.i.a. Principle 5.2.i.b would, for example, allow a social security institution investigating fraud in the social security sector to have access to relevant police data if the data are essential to its inquiry. It is recognised that the sort of public bodies referred to in paragraph 59 engage in activities which are similar in some ways to police activities and information held by the police may be of value to those activities. The notion of compatibility referred to in Principle 5.2.i.b reflects Article 5.b of the Data Protection Convention and therefore data may only be communicated for such related activities. The "legal obligations" of the police are to be interpreted in accordance with domestic law.

62. Principle 5.2.ii sets out two additional circumstances justifying communication, and it will be recalled that they will only "exceptionally" allow communication. By way of illustration of a, it may be the case that a social security office, faced with a claim for benefit presented by a migrant, may need to verify the latter's legal status in the country concerned by consulting a police file. This would also be in the interest of the claimant. It will be noted that the danger referred to in b must be both serious and imminent. It was thought appropriate to qualify the danger in this way given that Principle 5.2.ii is only concerned with exceptional cases justifying communication. Where a serious but non-imminent danger exists, communication could take place in accordance with the provisions of Principle 5.2.ii.a.

63. It may occasionally be necessary for the police to communicate data to private bodies, although not on the same scale as envisaged in the case of mutual assistance between the police and other public bodies. Sometimes the police will make data available on known confidence tricksters to shops and banks, or information concerning stolen credit cards and cheques. Once again, Principle 5.3 treats these as exceptional cases, requiring a clear legal obligation or authorisation (for example the consent of a magistrate), or the consent of the supervisory authority. In the absence of these factors, Principle 5.3 repeats the same conditions set out in Principle 5.2.ii.

64. It is to be understood that the provisions of Principles 5.2 and 5.3 cover the diffusion or broadcasting to public bodies or private persons of Identikit pictures or photographs of suspected persons which result from automated data processing.

65. Principle 5.4 relates to the international transfer of police data in the strict sense between police bodies. The reference to international law refers not only to international agreements concerning mutual assistance in criminal matters but also to co-operation within the framework of Interpol. In addition, this principle also takes account of the existence or conclusion of agreements between neighbouring states which are designed to improve transfrontier data communication between police bodies.

66. As regards the term, "police bodies", it is recognised that in certain member states certain types of police work may be carried out by authorities which are not stricto sensu "police bodies". Alternatively, it may be the case that certain functions which are thought to be within the competence of the police in certain member states may actually be discharged by non-police agencies in other member states.

67. For the purposes of Principle 5.4, therefore, the term "police bodies" should be understood in a broad sense. The question to be asked is whether the body is performing a function related to the prevention or suppression of criminal offences or to the maintenance of public order. Finally, Principle 5.4 should not be interpreted as excluding the possibility that data may be transferred to foreign judicial authorities where such authorities exercise functions concerning the prevention and suppression of criminal offences. It goes without saying that the requirements laid down in Principle 5.4 must be respected.

68. International communication of personal data between police bodies should only take place in accordance with the conditions set out either in a or b. Principle 5.4.b will be operative if the recipient state is not a member of Interpol or if there does not exist a treaty authorising communication of data to the recipient.

69. The text of Principle 5.4 reflects to some extent the provisions of Article 12 of the Data Protection Convention which treats the issue of transborder data flows. It will be noted that the clause "and provided that domestic regulations for the protection of the person are not prejudiced" is a counterpart to the concept of "equivalent protection" in the recipient state contained in paragraph 3.a of Article 12. Accordingly, the sending authority should satisfy itself as to the level of data protection for police data existing in the receiving state. Should the sending authority impose conditions on the use of the data in the receiving state (for example as to the length of conservation), it is to be understood that these conditions are to be respected. Both Principles 5.4.a and b are governed by the proviso.

70. Principle 5.5 sets out a number of rules which should govern the different forms of communication referred to above.

In addressing the rules which should govern the communicating of data, the drafters were inspired to some extent by the provisions contained in the "Rules on international police co-operation and on the internal control of Interpol's archives". In addition, the provisions of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 are reflected in the text.

71. The criteria outlined in Principle 5.5.i are aimed at ensuring that the communication of data can be justifiably carried out. It will be recalled that Principle 5.1 obliges a police body requesting data from another police body within the police sector to have a legitimate interest in obtaining the data. However, Principle 5.5.i envisages both internal and international exchanges of data being made subject to a justification requirement.

72. It is accepted however that domestic law or provisions in international agreements may dispense with the requirement of a reasoned request.

73. Principle 5.5.ii is not absolute in nature. The conditions set out are "as far as possible" to be satisfied. For example, it is accepted that in certain countries judicial decisions are not always relayed back to the police.

74. As stated previously, it is in the interest of both the police itself as well as the individual that data are accurate.

75. Principle 5.5.ii is flexible to the extent that it is appreciated that different monitoring periods exist in the various countries. It is for this reason that verification of the quality of data is made possible right up to the moment of communication.

76. Principle 5.5.iii may exceptionally allow the data to be used for purposes other than the purposes justifying the initial request for communication. It is essential that the communicating body be informed of an intention to so use the data. It must be borne in mind that the different purposes must relate to one or more of the factors contemplated in Principles 5.2 to 5.4.

77. Principle 5.5.iii does not apply to communication within the police sector. The rules outlined in Principles 4.1 and 5.1 are applicable to that case.

78. While Principle 2 constitutes a general principle for the collection of data by the police, Principle 5.6 concerns the particular situation where the police may seek to collect data by linking up its files with files held for different purposes, for example social security bodies, passenger lists kept by airlines, trade union membership files, etc. Alternatively, it may be sought to match up a number of files to see if they provide a clear profile of a certain type of delinquency and the sort of persons likely to engage in such delinquency.

79. The legitimacy of such practices is made conditional on the grant of either of the types of authorisation laid down in a and b. The "clear legal provision" referred to in Principle 5.6.b should state the conditions under which interlinkage can take place.

80. The possibility of the police having a direct computerised access to files held by different police bodies or by other bodies is discussed in the final sub-paragraph of Principle 5.6. Direct access in these circumstances must be in accordance with domestic legislation which should reflect certain key principles of the Recommendation.

Principle 6 - Publicity, right of access to police files, right of rectification and right of appeal

81. The requirement of publicity for the existence of police files as well as in regard to the rights of individuals vis-à-vis police files is of fundamental importance. Principle 6.1 entrusts the task of publicity to the supervisory authority, although member states will no doubt find additional ways of implementing this requirement.

82. The requirement of publicity should apply in principle to all automated files. However, it is recognised that the amount of information which can be given to police files will depend on particular circumstances.

For example, a more general description could be given to an ad hoc file related to a delicate inquiry in progress.

83. The individual should in the first instance be enabled to direct a request for access to a police file to the controller of the file. At the very least, this right should be exercised through the intermediary of the supervisory authority. Domestic law should determine the appropriate means of exercising the right. In addition, Principle 6.2 seeks to guarantee access by the data subject at reasonable intervals and without undue delay.

84. In principle, requests for access to data should not be registered as registration of requests could inhibit exercise of the right. However, if a member state does operate a system of registration, care should be taken to ensure that the register of requests is kept separate from the normal criminal files held by the police. Consideration should also be given to the destruction of the register after the lapse of a reasonable period of time.

85. Where data have been shown to be inaccurate as a result of the exercise of the right of access or found to be inaccurate, irrelevant or excessive as a result of the application of other principles, Principle 6.3 provides that the police should ensure that the relevant file is put in order. This can be done by erasing inaccurate data, or rectifying the information so as to make it correspond to the rightful situation. As an alternative to erasure, Principle 6.3 makes it possible for data to be retained on the file but subject to an accompanying statement which sets out the true position. This could be the case, for example, for statements made by witnesses which have been shown to be inaccurate. Rather than removing the statement entirely from the file, it may be desirable to retain it while at the same time attaching a true version of events.

86. The second sub-paragraph of Principle 6.3 sets out a timetable for erasure or for corrective measures to be taken. It is to be noted that these precautions are not confined

to the file itself, but must, as far as possible, be applied to every other document linked to the file.

87. Experience in at least one member state has shown that in principle it should be possible to authorise access in the vast majority of cases. Principle 6.4 recognises that the right of access (and thus the rights of rectification and erasure) may be refused in the cases set out.

88. It will be noted that the restriction in favour of the data subject or the rights and freedoms of others has been taken over from Article 9, subparagraph 2.b of the Data Protection Convention. In the context of the police sector, this expression could cover the need to protect witnesses or police informers.

89. The alternative justification for restricting access - "indispensable for the performance of a legal task of the police" - does not have an exact counterpart in Article 9 of the Convention. However, it is believed that, within the context of the restrictions on the right of access, the Convention derogation for "the suppression of criminal offences" is best interpreted along those lines.

90. An individual may be pressurised into obtaining a copy of his police file, for example by a prospective employer. It may not be in his interests to receive a written copy or a statement of what is contained in the file. In such a case, domestic law may authorise oral communication of the file contents.

91. Principles 6.5 and 6.6 set out certain procedural guarantees in the event of a refusal or restriction of the rights of access, rectification or erasure. In the first place, a refusal or restriction must be motivated in writing. It is important to demonstrate that the duty conferred on the police by Principle 6.4 - to weigh the rights of the data subject against the superior interests stated therein - has been exercised.

92. It will be noted that communication of the reasons may only be denied for the same reasons that justify a refusal or restriction of the rights of access, rectification or erasure. The data subject should be told of his right to appeal against a refusal of access. This right should be stated in the reasoned decision envisaged in Principle 6.5. However, even if no reasons are given for a refusal of access, because a superior interest is thought by the police to be at stake, information should still be given to the individual on how to challenge the decision.

93. Principle 6.6 is drafted in such a way as to take account of the different practices in the various member states in regard to the exercise of the right of access. In certain countries it may be the case that the individual will have no direct right of access to a police file and he will be obliged to gain access through the intermediary of the supervisory authority.

94. The reference to "or another independent body" indicates that in certain countries a court or tribunal may replace the supervisory authority for appeal purposes. But

irrespective of this possibility, the data subject will of course enjoy the right to go to a court or tribunal to seek rectification of a file, or completion of a file, etc where this has been refused.

95. Domestic law will determine the interventionist powers of the supervisory authority or other independent body in regard to the examination of the contested police file. It may be that the inspecting body is not obliged to actually communicate the data to the individual even if there is no justification for refusing access. The data subject could be simply informed that a verification of the police file has taken place, and that the file is in order. Alternatively, the inspecting body may decide to release the data contained on the file to the data subject.

Principle 7 - Length of storage and updating of data

96. It is essential that periodic reviews of police files are undertaken to ensure that they are purged of superfluous or inaccurate data and kept up to date. Principle 7.1 lists certain considerations which should be borne in mind when determining whether or not data continue to be necessary for the prevention and suppression of crime or for the maintenance of public order.

97. Principle 7.2 expresses the desire that the quality of the data should be regularly checked pursuant to fixed rules and that data should also be the subject of rule-based conservation periods. Implementation of this principle would facilitate the task conferred on the police by Principle 5.5, sub-paragraph ii.

98. Domestic law may authorise the means for laying down such rules. Alternatively, rules could be formulated by the supervisory authority itself in consultation with police bodies. Should the police itself elaborate rules, the supervisory authority should be consulted as to their content and application.

99. It is accepted that police data are of obvious value for research and statistical purposes. Domestic laws on archives will provide ways of dealing with any problems which arise in this context. Where relevant, reference should also be made to the provisions of Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics.

Principle 8 - Data security

100. Principle 8 reflects the requirements of both physical security and confidentiality. The responsible body referred to previously should ensure that only specifically authorised personnel have access to terminals and that communications of data carried out pursuant to requests made under Principle 5 are authorised. For this purpose, a log could possibly be kept by the responsible body recording the sort of information contemplated in Principle 5.5.i.

Footnote

When this Recommendation was adopted:

- in accordance with Article 10.c of the Rules of Procedure for the meetings of the Ministers Deputies, the Representative of Ireland reserved the right of his Government to comply with it or not, the Representative of the United Kingdom reserved the right of her Government to comply or not with Principles 2.2 and 2.4 of the Recommendation, and the Representative of the Federal Republic of Germany reserved the right of his Government to comply or not with principle 2.1 of the Recommendation;

- in accordance with Article 10.2.d of the said Rules of Procedure, the Representative of Switzerland abstained, stating that he reserved the right of his Government to comply with it or not and undelining that his abstention should not be interpreted as expressing disapproval of the Recommendation as a whole.

By letter of 10 December 1997, the Irish Government notified the Secretariat of its decision to limit the reservation made at the time of the adoption of the Recommendation to three provisions thereof, viz., Principle 2.2, Principle 2.3, and Principle 2.4