COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 1 June 2004 T-PD (2004) 07

RECOMMENDATION NO.R (87) 15 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR

FIRST EVALUATION

SECOND EVALUATION

THIRD EVALUATION

Secretariat memorandum
prepared by the
Directorate General of Legal Affairs

TABLE OF CONTENTS

The international legal instruments of the
Council of Europe in the field of data protection
can also be found in electronic version on
the data protection website at
www.legal.coe.int/dataprotection/

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

---

RECOMMENDATION NO. R (87) 15
OF THE COMMITTEE OF MINISTERS TO MEMBER STATES
REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR[1]

(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.

---

[1] 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 Governement 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 Governement 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

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.

First evaluation of the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector, done in 1994

CONTENTS

AD HOC TERMS OF REFERENCE

1.	Name of the Committee:	PROJECT GROUP ON DATA PROTECTION (CJ-PD)
2.	Source of terms of reference:	Decision No. CM/547/180193 of the Committee of Ministers
3.	Completion date:	December 1994
4.	Terms of reference:	

To evaluate the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector and, in particular the need to revise the text, namely its scope and principle 5.4 (international communication), bearing in mind the principles set out in Assembly Recommendation 1181 (1992).

5.	Other Committee to be informed of terms of reference:	Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD)

THE CJ-PD'S CONCLUSIONS

6. The Project Group reached the conclusion that Recommendation No. R (87) 15 gives adequate protection for personal data used for police purposes and that, at this stage, there is no need to revise it, or parts of it.

7. The Project Group felt that Article 5.4 of Recommendation No. R (87) 15, especially when read together with paragraphs 56-80 of the Explanatory Memorandum, appears flexible enough to meet the present and foreseeable requirements of international agreements on the exchange of data for police purposes.

8. In view of:

i) the gradual and on-going increase of member States' ratification of Convention 108;

ii) the on-going, gradual and occasionally uneven adoption by member States of the principles set out in Recommendation No. R (87) 15;

iii) the reference to Recommendation No. R (87) 15 in international agreements such as the Schengen Agreement;

iv) the implementation of new systems for the sharing of personal data used for police purposes, such as EUROPOL;

v) the rapid development of new technologies;

vi) the concerns expressed by both the Parliamentary Assembly and the Committee of Ministers;

the Project Group proposes that the relevance of Recommendation No. R (87) 15 should become the subject of periodic review on a regular rather than an ad hoc basis. For this purpose it is further proposed that the next review be carried out and reported on by December 1998 and thereafter on a four-yearly basis.

REPORT

i) INTRODUCTION

9. On 17 September 1987 the Committee of Ministers adopted Recommendation No. R (87) 15 regulating the use of personal data in the police sector (Appendix B to the present report).

10. In its Recommendation 1181 (1992) on police co-operation and protection of personal data in the police sector (Appendix C to the present report), the Parliamentary Assembly recommended that the Committee of Ministers, among other things, draw up a convention enshrining the principles laid down in Recommendation No. R (87) 15.

11. During its 478th meeting (June 1992), the Committee of Ministers adopted Decision No. CM 537/220692 entrusting the Project Group with the drawing up of an opinion on the Assembly's Recommendation 1181.

12. During its 24th meeting (22-25 September 1992), the Project Group drew up the Opinion which appears in Appendix D to the present report.

13. At the same time the Committee of Ministers also requested the opinion of the Consultative Committee of Convention 108. The text of the Consultative Committee's opinion appears in Appendix E to the present report.

14. In the light of these Opinions, the Committee of Ministers, at its 486th meeting of the Ministers' Deputies (January 1993), adopted Decision No. CM/547/180193, entrusting the Project Group with the ad hoc terms of reference which appear above.

ii. SUMMARY OF THE WORK DONE

15. At its 25th meeting (11-14 May 1993) the Project Group took note of the ad hoc terms of reference with which the Committee of Ministers had entrusted the CJ-PD.

16. In a first exchange of views several experts drew attention to the danger that a general revision of Recommendation No. R (87) 15 might lead to some of its principles being weakened. They argued that rather than a systematic revision of the various provisions, new technologies used by the police (eg. satellite surveillance) should be examined and, if appropriate, additional principles be defined. Other experts referred to the growing number of structures for the exchange of police information, such as Interpol, Europol, the Channel Tunnel agreements and customs agreements.

17. Experts undertook to present in writing before 1 September 1993 a short report on the implementation, in their country, of Recommendation No. R (87) 15 and on the main problems met in the implementation, as well as, if appropriate, suggestions for revision of the provisions in particular those on the scope and on international communication.

18. Reports were received from the experts of the following countries:

Austria	Italy
Belgium	Luxembourg
Bulgaria	Norway
Denmark	Portugal
Finland	Spain
Germany	Sweden
Greece	Switzerland
Hungary	United Kingdom

19. During its 26th meeting (19-22 October 1993), the Project Group accepted the offer made by the expert from Malta, Mr J. CANNATACI, to draw up a report synthesising the experts' written observations and any other information available, in particular with regard to implementation of the Recommendation, its scope and questions in connection with international communication.

20. The report, presented by the rapporteur on 10 March 1994, appears in Appendix F to the present report.

21. During its 5th meeting (22-25 March 1994), the Bureau of the Project Group amended the report of the Rapporteur's conclusions slightly and decided to submit them to the Project Group for approval.

22. At its 27th meeting (21-24 June 1994), the Project Group considered and approved the present Final Activity Report.

APPENDIX A

RECOMMENDATION 1181 (1992)[1] ***on police co-operation and protection of personal data in the police sector***

1. As a result of the Schengen Agreement, the European states co-operating in that agreement will proceed with the exchange of automatically processed personal data in the police sector. It is most likely that such an exchange will cover the whole of the European Community after the disappearance of frontier controls at its internal borders.

2. Nowadays there is already an intensive exchange of data in the police sector among Council of Europe member states on a bilateral or multilateral basis and through Interpol.

3. It is of vital importance for an efficient combat against international crime that it is fought at national and at European level.

4. An efficient fight against crime implies an exchange of data in the police sector.

5. In this respect it is useful to recall the Assembly's Recommendation 1044 (1986) on international crime and its plea for a European information and intelligence centre (Europol), and Recommendation No. R (87) 15 of the Committee of Ministers to member states of the Council of Europe regulating the use of personal data in the police sector.

6. It is necessary, however, that there be adequate protection of personal data in the police sector and one may note with satisfaction that the Council of Europe concluded, in 1981, a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. However, in order to be fully effective, it is not sufficient that this convention has, to date, only been ratified by eleven member states.

7. The Assembly therefore recommends that the Committee of Ministers :

i. draw up a convention enshrining the principles laid down in its Recommendation No. R (87) 15 ;

ii. promote the application of these principles in the exchange of data in the police sector between member states and between member states and third countries via Interpol. In this respect the implementation of the following principles is of the utmost importance :

a. data should be accurate, relevant, not exceed the purpose for which they are stored and, where necessary, kept up to date ;

b. they should be screened before they are stored ;

c. an individual should have the right to know whether personal data concerning him are kept ;

1 Text adopted by the Standing Committee, acting on behalf of the Assembly, on 11 March 1992. See Doc. 6557, report of the Committee on Legal Affairs and Human Rights, Rapporteur : Mr Stoffelen.

d. he should have an appropriate right of access to such data ;

e. he should have the right to challenge such data and, if necessary, have them rectified or erased ;

f. individuals who are denied access to files relating to them should have a right to appeal to an independent authority which has full access to all relevant files and which can and should weigh the conflicting interests involved ;

g. there should be an independent authority outside the police sector responsible for ensuring respect of the principles laid down in such a convention ;

iii. appeal to member states to ensure that data in the police sector may only be exchanged with other member states and with Interpol on the lines provided for in the proposed draft convention.

APPENDIX B

Opinion formulated by the Project Group on Data Protection

i. to draw up a convention enshrining the principles laid down in its Recommendation No R (87) 15

1. The Project Group on Data Protection shares the concern of the Parliamentary Assembly that with a view to the increasing exchange of personal data in the police sector, to combat international crime, an adequate protection of these data is necessary. This is the more important, now that a growing number of agreements between European States call for international co-operation not only between national police forces but also between other national authorities in the fields of border control, asylum and refugees, in the absence sofar, at least outside the European Community, of uniform guarantees for the protection of personal data, which these police forces and other authorities may be required to exchange in the framework of their co-operation.

2. The Project Group has carefully examined the legal and practical consequences of the implementation of the Assembly's recommendation under sub-paragraph 7 i. to draw up a convention enshrining the principles laid down in Recommendation No R (87) 15.

3. In respect of sub-paragraph 7 i., the Project Group has identified three options:

(a) to draw up a new convention

The Project Group recalls the essential role of Convention 108, as the main legal instrument for the implementation of one of the elements of the right on privacy laid down in Article 8 of the Human Rights Convention, and as the cornerstone of the protection of personal data at international level.

The Project Group is of the opinion that, apart from the time needed for the elaboration and ratification of a new convention, ratification of Convention 108 as the basis of data protection in general would seem to be a prior condition for the ratification of any further Council of Europe convention in the field of data protection.

(b) to amend Convention 108

Article 19 (c) of the Convention entrusts the Consultative Committee with the formulation of an opinion on any proposal for amendment.

However, the Project Group wishes to draw the attention to the general nature of Convention 108, which has been designed to ensure respect of a number of basic principles in all sectors where personal data are collected and automatically processed.

(c) to conclude an Additional Protocol to Convention 108

Again, the Project Group refers to the opinion to be given on this option by the Consultative Committee. However, the Project Group accepts that the definition, by means of an Additional Protocol to Convention 108, of basic rules for the protection of personal data in the exchange of

information between national authorities would be useful for all States which have not yet adequate legislation on such exchange.

4. In the light of the observations under paragraph 3 above, the Project Group has defined a fourth option, consisting of establishing on short term such basic rules by means of a Recommendation of the Committee of Ministers. In this respect, it recalls that although not mandatory, these legal instruments are less rigid in nature, take generally less time to draw up, and are easier to adapt to changing circumstances.

5. The Project Group recalls the important role which Recommendation No R (87) 15 has played and still plays in the protection of personal data in the police sector. Reference to Recommendation No R (87) 15 is made in, among other texts, the Schengen Agreement and the provisions on the creation of EUROPOL, the European Information System and the Customs Information System.

6. The Project Group agrees that at this stage, rather than to elaborate a new convention, Recommendation No R (87) 15 should be examined carefully, and an assessment made of the need to revise, in particular, the scope of the Recommendation and principle 5.4 (international communication) with a view to ensuring an adequate protection of those personal data kept by police forces and other national authorities in the fields of border control and customer services, asylum and refugees and which are the subject of transborder data flows, or which are registered in supranational data banks.

In the long term, the elaboration of a conventional text could be considered.

ii. to promote the application of the principles in Recommendation No R (87) 15

7. Most experts in the Project Group fully endorse the recommendation that the application of these principles be promoted. In this light, the Group suggests that the possibility be examined to assess, on a regular basis, implementation of these principles.

iii. appeal to member States to ensure that data in the police sector may only be exchanged with other member States and with Interpol on the lines provided for in the proposed draft convention

8. The Project Group refers to its opinion expressed in paragraph 6 above.

APPENDIX C

Opinion formulated by the Consultative Committee

1. The Consultative Committee has examined Recommendation 1181 of the Parliamentary Assembly, bearing in mind also the conclusions reached by the Project Group on Data Protection in respect of the same Recommendation.

2. The Consultative Committee endorses the conclusions of the Assembly's Rapporteur, that in the fight against international crime co-operation between police forces is increasing, resulting in steadily growing transborder flows of data, including personal data. Under Article 12 of Convention 108 these transborder data flows require respect of regulations providing equivalent protection of personal data.

3. In this respect the Consultative Committee underlines that Article 12 applies to any transborder data flow, in the private sector as well as in the public sector, and not only to the transfer of personal data from one national police force to the other, but between all public authorities.

4. The Consultative Committee recalls that Convention 108 and in particular its Article 12 have been designed to apply to the protection of personal data wherever such data are being collected and processed. The strategy which hitherto has been followed by the Council of Europe in the field of data protection implies that Convention 108 lays down the general principles and that these principles are subsequently elaborated for each of the different sectors by means of recommendations of the Committee of Ministers.

5. Whilst it is true that in the police sector a number of international agreements - both bilateral and multilateral - are being concluded, which may have consequences for the protection of personal data which by virtue of these agreements may be subjected to transborder communication, the Consultative Committee agrees that at this stage, this transborder communication does not require the immediate elaboration of a new international compulsory instrument, mainly for the following reasons:

a. in general, these international agreements take account of data protection requirements, and in most cases refer to the relevant Council of Europe texts;

b. the elaboration of a new legal instrument can be efficiently undertaken, only when sufficient experience is available on the implementation of the international co-operation agreements;

c. Convention 108 - which will remain the basic instrument in the area of data protection - is still being ratified by a number of member States.

6. The Consultative Committee shares therefore the opinion of the Project Group that at this stage Recommendation N° R (87) 15 regulating the use of personal data in the police sector should be examined carefully. An assessment should be made of the need to revise, in particular, the scope of the Recommendation and principle 5.4 (international communication) with a view to ensuring an adequate protection of those personal data kept by police forces and other national authorities in the fields of border control, customs services, asylum and refugees and which are the subject of transborder data flows, or which are registered in supranational data banks.

7. Under its responsibility for facilitating or improving the application of Convention 108, the Consultative Committee will monitor protection of personal data in the implementation of the various

international agreements on co-operation between police forces or other national authorities. It will also consider the results of the assessment of Recommendation N° R (87) 15, if the Committee of Ministers were to follow the opinion of the Project Group.

8. When sufficient information is available on the practical implementation of the international co-operation agreements, and in the light of the results of the assessment, if any, of Recommendation N° R (87) 15, the Consultative Committee will consider whether Convention 108 and in particular its Article 12 still provide sufficient guarantees for the protection of personal data subjected to transborder data flows. If the Committee would not be satisfied, it might envisage the possibility of elaborating additional rules to improve this protection.

9. The Consultative Committee confirms, however, that whatever the results of such considerations, Convention 108 should not be amended; if additional rules were to be established, they could be the subject of an Additional Protocol to the Convention.

Such Additional Protocol would enable those Parties to Convention 108, who would wish to do so, to complement the existing provisions on transborder data flows, without changing their basic undertakings under Convention 108. Nor would the Protocol prevent other States from becoming a Party to Convention 108 only.

APPENDIX D

Report by Mr J. CANNATACI, expert from Malta

1. This Report is NOT a synopsis of the national reports submitted but IS a summary of the qualitative analysis performed on all the national reports in question. As such, the qualitative analysis set out to answer the following questions:

i. Response Overview: which are those articles of Recommendation R (87) 15, including those not specifically indicated in the terms of reference by the Committee of Ministers, which member States felt may benefit from revision and/or clarification?

ii. Classification of Response: if one were to apply a simple classification to the response from member States, which responses indicated clarification (C) as opposed to radical review (R), strengthening of the provisions (S) or weakening of the provisions (W)?

iii. Critical Level of Response: is the level of revisionary response received sufficiently different from that existing in 1987 (ie. at the time of the finalisation of R (87) 15) and is it sufficiently high to warrant revision of the Recommendation, given all the diversion of resources that such a revision would entail?

iv. Specific relevance of Art. 5.4: Is Article 5, read together with the Explanatory Memorandum, adequate in achieving the balance between sufficient protection of the individual on the one hand and extensive exchange of data between police forces on the other hand?

2. The results of the answers to the questions outlined in 1.i and 1.ii above may be surveyed in the chart illustrated in Fig. 1 below. At a glance, readers may understand that the majority of the member States did not suggest either radical review (R) or Weakening of the provisions (W), most responses were aimed rather at further clarification (C) and occasionally strengthening (S). This reinforces the impression gained from listening to the national experts during plenary sessions that Recommendation R (87) 15 continues to provide a sound basis for data protection in the police sector. Moreover, a closer investigation of the requests for clarification would indicate that the current text of R (87) 15 is sufficiently elastic to permit the various interpretations that some member States may wish to see specifically mentioned in the text or, more often, in the Explanatory Memorandum. Very often these requests are made "for the avoidance of doubt" rather than the "absolute certainty that the Recommendation stipulates a prohibition or mandates a requirement." The very fact that the current text is supple enough to meet the various needs of different member States would militate more in favour of maintenance of the current text rather than the re-opening of the Pandora's box that re-formulation of the text may bring about.[1]

3. The analysis illustrated in Fig. 1 clearly shows that the bulk of the suggestions for revision of R (87) 15 come from only two member States: Germany and the United Kingdom. This is a very important consideration in a determination of the Critical Level of Response mentioned in 1.iii above. This would suggest that very little has changed since 1987; both Germany and the United Kingdom remain, together with Ireland, (Switzerland has since re-considered its position) the member States who entered Reservations to Art. 2 of R (87) 15 when the Recommendation was adopted in 1987. The reservations entered by Germany and the United Kingdom in 1987 are maintained in 1993 with some

1. Those experts who, like the Rapporteur, formed part of the Project Group in 1986-87, will recall the very strenuous negotiations required to arrive at a consensus basis for the current text. Such memories do not favour re-opening discussions on the text except for very serious reasons.

further additions: the bulk of the United Kingdom's remarks are aimed at further clarification while those of Germany contain the largest number of proposed revisions which would effectively weaken the Recommendation. This consideration compares with the sentiments expressed by the majority of the other respondents: ie that R (87) 15 does not pose any serious problems or that "Several experts concur that the provisions of the Recommendation constitute an inalterable necessary minimum" (CJ-PD (93) 48). This view is typically expressed in the strongest terms by the Swiss Federal Data Protection Officer who "takes the view that these Regulations should not be weakened under any circumstances and that the principles set out in Recommendation R (87) 15 should be regarded as established".
In this respect therefore, and given "the lifting of Switzerland's reservations regarding Recommendation N° R (87) 15" the position in 1993-94 would appear to have moved closer towards an even greater consensus on the text of R (87) 15 than that which existed in 1987, with the German and U.K. positions on this subject becoming increasingly more lonely.

4. As indicated in Fig. 1, the number of requests for serious revision of the text, whether to strengthen or to weaken the provisions, is too small to merit a re-opening of the discussion on R (87) 15 as a priority matter for the Project Group on Data Protection.

5. The considerations outlined in paras. 2, 3 and 4 above would suggest that the arguments to retain the status quo over the text of R (87) 15 would appear to be stronger than those which favour re-opening of detailed discussion of the text and its explanatory memorandum.

6. The attention of the Rapporteur was drawn directly to Article 5.4 by the Terms of Reference. The concern expressed with respect to this principle is typified by the comments of the United Kingdom expert: "The United Kingdom believes that paragraph 5.4 needs to be reviewed in detail in the light of continuing work on the development of international agreements about the exchange of data for police purposes." A similar observation is to be found in the Swiss response: "The application of the Recommendation to customs authorities who have access to police data systems should be examined. Principles should also be formulated on exchange of data between different police systems". Like the United Kingdom comments, the Swiss do not elaborate as to why the current formulation of 5.4 may be problematic, so in search of a further understanding of a difficulty one turns to the other two member States who made specific reference to 5.4 in their responses: Belgium and Germany. Both of these countries had no really serious difficulties with 5.4. Belgium sets the tone: "The provisions contained in the current text of the Recommendation should be regarded as laying down the minimum level of data protection which cannot be called into question. Consequently these provisions can only be made more explicit or practical rules added where this proves necessary. Accordingly, new details could be added to Principles 5.4 (international communication)...". It is important to make the distinction between those changes which are strictly necessary and those which are merely desirable. Belgium clearly makes this distinction, calling for changes "where this proves necessary", but indicates only the possible addition of "details". Likewise, the German remark is not radical but simply one of clarification: "In view of the fact that the Interpol statutes as the basis for co-operation within the framework of Interpol do not have the force of a law, N° 5.4 lit. a. should be worded as follows so as to avert potential misunderstandings on account of the existing wording: "if there exists a legal provision to this effect under national law or international agreements".

Given the scarcity of detail in the comments reproduced above, it is difficult to understand why the texts of 5.4, when read together with the remainder of Principle 5 and the accompanying Explanatory Memorandum, are not supple enough to satisfy the countries concerned. It is felt that the following excerpts from R (87) 15 require no further explanation:

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 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.

5.4 International Communication

Communication of data to foreign authorities should be restricted to police bodies. It should also 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 provision 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.

The problems expressed by member States over "international co-operation" and "Interpol" would appear to be resolved by the following explanations given within the Explanatory Memorandum:

"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.

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 to Interpol. In addition, this principle also takes account of the existence or conclusions 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 type of police work may be carried out by authorities which are not strictu 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."

Thus, whether "police bodies" or "public bodies", none of the data exchange needs mentioned by various member States would appear to be beyond the scope of Article 5 of R (87) 15. Nor would the wording of the current provisions appear to be so lax as to arouse undue concern at the opposite end of the data protection scale. As explained in paragraph 56 of the Explanatory Memorandum, "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". It is submitted that no overwhelming arguments have been advanced to date as to why current formulation of Principle 5 and its accompanying Explanatory Memorandum fail in providing the most balanced formula capable of providing equitable provision for current requirements.

In the light of the foregoing, it is difficult to find convincing arguments which highlight why it is really necessary (rather than being possibly - and arguably - desirable) to amend Recommendation R (87) 15. Before such convincing arguments are advanced, it is difficult to abandon the principle of "Leave well alone".

Figure 1

Comparative Analysis: National Responses to Recommendation R (87) 15 – POLICE

R (87) 15 Art. No.	United Kingdom	Germany	Finland	Belgium	Austria	Hungary	Norway	Switzer-land
Scope Definition	C			C	C	C		
1.1		C						C
1.2	C							
1.3								
1.4		R/W	C					
2.1	R/W	R						
2.2	R	R						C
2.3								
2.4	R						C	C
3.1								
3.2	C	C					C	C
3.3								
4.	C							
5.1		C		C				
5.2i								
5.2ii		R/W						
5.3i								
5.3ii		R/W						
5.4	R	C		C				
5.5		R/W		C				
5.6	C	C		C				
6.1								
6.2								
6.3								
6.4								
6.5								
6.6		C						
7.1			S					
7.2								
8	C							

C=Clarify; S=Strengthen; W=Weaken; R=Radical Review/Reservation

(The following states responded but did not recommend amendments to specific sections: Luxembourg, Sweden, Italy, Spain, Denmark, Greece, Bulgaria)

Law & Information Technology Research Unit – University of Malta - 1994

Second evaluation of the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector, done in 1998

CONTENTS

I. AD HOC TERMS OF REFERENCE

1.	Name of the Committee:	PROJECT GROUP ON DATA PROTECTION (CJ-PD)
2.	Source of terms of reference:	Decision No. CM/547/180193 of the Committee of Ministers and Decision of 7-8 February 1995
3.	Completion date:	December 1998

4. Terms of reference:
To evaluate every four years the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector.

5. Other Committee to be informed of terms of reference:

Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD)

European Committee on Crime Problems (CDPC)

Committee of Experts on Police Ethics and Problems of Policing (PC-PO)

II. THE CJ-PD'S CONCLUSIONS

6. The Project Group reached the conclusion that Recommendation No. R (87) 15 gives adequate protection for personal data used for police purposes in the fields which it covers which were relevant at the time of its adoption.

7. It is proposed that the CJ-PD, in particular in consultation with the CDPC, be instructed to consider the question of whether the application of the principles of Recommendation No. (87) 15 to present-day police and judicial practices in combating crime requires the adoption of a supplementary legal instrument to this recommendation.

8. The following points mentioned in the appended report should be taken into consideration for future work:

- the identification of targets of criminal intelligence, either in a substantive way, defining criteria in the law, or in a procedural way, defining the authorities and the circumstances that can give rise to the collection of criminal intelligence;

- the time limit for storing criminal intelligence data after which the data should be reviewed or deleted;

- the use of data about unsuspected persons, collected in the course of the investigation of a specific offence, for the investigation of other unrelated offences;

- the matching of data from open sources, such as the Internet or public files, with police data in order to find data about persons who were not suspected beforehand;

- the notification of the persons about whom data are stored by the police;

- the storage and use of genetic data with a view to the identification of criminals;

- the establishment of a supervisory authority for the protection of personal data held by the police;

- instruments for monitoring development in the use of investigative methods involving the collection, storage and use of personal data.

III. REPORT

i) INTRODUCTION

9. On 17 September 1987 the Committee of Ministers adopted Recommendation No. R (87) 15 regulating the use of personal data in the police sector (Appendix B to the present report).

10. In its Recommendation 1181 (1992) on police co-operation and protection of personal data in the police sector (Appendix C to the present report), the Parliamentary Assembly recommended that the Committee of Ministers, among other things, draw up a Convention enshrining the principles laid down in Recommendation No. R (87) 15.

11. During its 478th meeting (June 1992), the Committee of Ministers adopted Decision No. CM 537/220692 entrusting the Project Group on Data Protection and the Consultative Committee of Convention 108 with the drawing up of an opinion on the Assembly's Recommendation 1181.

12. In the light of these opinions, the Ministers' Deputies, at their 486th meeting (January 1993), adopted Decision No. CM 547/180193, conferring on the Project Group the task of evaluating the relevance of Recommendation No R (87) 15 with a view to its possible revision.

13. The CJ-PD completed a first evaluation of the recommendation in 1994, which appears in document CJ-PD (94) 7.

14. In the light of this evaluation and the conclusions of the CJ-PD, the Committee of Ministers, at its 528th meeting (7 Feburary 1995), entrusted the CJ-PD with the ad hoc terms of reference which appear above.

ii. SUMMARY OF THE WORK DONE

15. At its 34th meeting (14-17 October 1997) the CJ-PD entrusted a rapporteur, Mr A. Patijn (Netherlands), with the drafting of a report on the evaluation of the recommendation, at the end of a period of four years, in accordance with the Committee of Ministers' decision (7 February 1995).

16. The draft report, presented by the Rapporteur at the 35th meeting of the CJ-PD (25-27 March 1998 and amended by him in the light of observations made during meetings of the Bureau and the CJ-PD which followed, appears in Appendix D to this report.

17. At its 36th meeting (28-30 October 1998), the Project Group considered and approved this Final Activity Report.

APPENDICES

APPENDIX A

Report by Mr A. PATIJN, Expert of the CJ-PD from the Netherlands

Data protection and the police. Evaluation of Recommendation R (87)15 regulating the use of personal data in the police sector

1. Background

The Committee of Ministers decided to review the Recommendation R (87) 15 regulating the use of personal data in the police sector (Decision CM/547/180193). The previous evaluation was accomplished in 1994 and appears in the document CJ-PD (94) 7. In that report, as adopted by the Committee of Ministers, it was established that the Recommendation be the subject of periodic review on a regular basis every four years. A next evaluation is to be accomplished in 1998. This paper is a draft evaluation to this end. (A previous draft was circulated in March 1998.) This version deals with reactions received from Belgium, Germany, Hungary, Ireland and the Netherlands.

In the meantime, the recommendation has been referred to in two international agreements. Article 115, first paragraph, of the Schengen Agreement states that control by the supervisory authority should take account of the recommendation. The Treaty of Amsterdam incorporated the Schengen Agreement into the EU Treaty. Likewise, in its article 14, paragraph 1, the Europol Treaty provides that processing of police data should take account of the 1987 recommendation of the Council of Europe. These two references would make it a complicated affair to change the contents of the recommendation. At least formally it would imply a change of both conventions. Up till now, no serious problems have been raised that would necessitate changing the recommendation. It is proposed therefore not to revise the recommendation.

The 1987 recommendation dealt with police data as perceived in the first half of that decade. Organised crime was not yet an issue of international concern. Criminal intelligence files were not as evolved as they are nowadays. At that time, the police held mainly data about the people they suspected of having committed a criminal offence. The information remained separate from the criminal records. Recommendation R (84) 10 of the Council of Europe on the criminal record and the rehabilitation of convicted persons deals more specifically with this last topic. Things have changed since then. This raises the question of whether an additional international instrument dealing with certain specific questions in more detail would be useful

Proposal: It is proposed that the Committee of Ministers change its original decision to evaluate the 1987 Recommendation periodically, to the effect that periodically the question be answered whether any additional international instrument should be formulated.

This report mentions elements that could be relevant in answering to the question whether an additional instrument would be desirable. It proposes that the Committee of Ministers recommend that national legislators explicitly deal with certain questions of data protection, either in the national Data Protection Act, the national Code of Criminal Procedure, or national or regional Police law.

2. General Remarks

There is an inherent but inevitable tension between police powers and human rights. Adequate police powers are necessary to allow the police to fulfil their tasks. For the present paper the combating of crime is the prevailing perspective. But these powers, to be adequate, necessarily interfere with the respect for private life and should therefore be restricted to the extent that is necessary. The balance between powers necessary for the police and the restrictions necessary to protect private life shifts continually with progressing information technology. This technology enables criminals to reach their goals more effectively; on the other hand it enables the police to fulfil their tasks more effectively. If they are not properly regulated though, the new abilities of the police might again affect the private life of ordinary citizens. Article 8 of the European Convention on Human Rights requires a legal basis in this case. Practical possibilities to use new technology should be accompanied by legal powers where the use of technology by the police interferes with private life. The tension between the availability of adequate police powers and the protection of private life thus becomes a creative force generating new law to safeguard the quality of life in our changing democratic societies.

At the national level first, the legislator should be continuously aware of this challenge. The pressing social needs are a factor to be weighed. In the area of crime, these differ nationally more strongly than in other areas of society. Secondly, at an international level, one could look for possibilities to harmonise rules if there appear to be common elements in the national law of the different countries of the Council of Europe.

These general remarks are valid for all sorts of interference in private life, such as searches in premises and the interception of telecommunications. Data protection is just one of them and does not constitute an exception; nor is it something special in this respect. It is this last aspect though that is the further topic of this paper.

Proposal: It is recommended starting with a list of points of awareness for national legislators, before trying to harmonise national approaches. In due course it will be seen whether it might be desirable to regulate, at the international level, certain elements that have evolved. This work should be done in close co-operation with the CD-PC, competent in criminal matters, since both areas of law are involved.

3. Are criminal data sensitive data?

The main new developments are in the area of criminal investigation. Personal data collected and processed in the performance of other police tasks, such as the maintenance of public order or the lending of help to those that need it, have not changed much during the period of evaluation. The recommendation seems to suffice for those data. An additional instrument with regard to data collected and processed for the purpose of suppressing criminal offences might however be considered. These data are further referred to in this paper as criminal data. Hereafter, this paper deals with criminal data only.

Should criminal data be regarded as sensitive? Article 6 of Convention 108 does not mention them as such. It only states that, with regard to data relating to criminal convictions, the same applies as to the other special categories of data that are generally referred to as sensitive data. This implies that these data may not be processed unless domestic law provides appropriate safeguards. This article is, however, restricted to criminal convictions. Criminal data about persons who are not yet convicted are not covered. One might question, though, whether in practice these data are often not even more sensitive, since no impartial tribunal has yet convicted a data subject on the basis of

legally collected evidence in accordance with article 6 of the Human Rights Convention. It goes without saying that in most cases, after a conviction, a person has a right of appeal. Since somebody's position in society may be affected by data based on suspicions even more than by data based on convictions, particularly when the data become known outside the police sector, criminal data in the wider sense, are, for the purposes of this paper, regarded as sensitive.

It should be recalled that the EU Directive 95/46 has a broader approach towards criminal data. In paragraph 5 of article 8 about special categories of processing, appropriate safeguards are requested for all data relating to offences, whether they relate to convictions, to suspected persons, criminal intelligence or to any other personal data collected during the course of a criminal investigation. The directive is applicable to subjects falling under the scope of community law, e.g. insurance companies that process criminal data about persons that have tried to deceive the company. The directive, however, is, having regard to article 3, paragraph 2, not applicable to police files as such. It is relevant again, for the purpose of this paper, where the question arises whether data from processing falling under the scope of the directive, may be communicated to the police. E.g. under paragraph 6 hereafter the use of public files for police purposes is discussed. Since most public files fall under community law, the processing of the data they contain for police purposes should, within the European Union, be judged against the background of article 13, paragraph 1, under d, of the directive.

4. Several areas of law and the purpose of this paper

Recommendation No. (87) 15 on police data is intended to make the principles of Convention 108 more concrete with regard to the police sector. In most countries that have ratified Convention 108 and therefore have data protection rules in force, the police sector is covered by these general rules. Some countries have specific data protection rules for the police sector. The rules for collection of data usually find their origin in the Code of Criminal Procedure or in a specific Act regulating the police. These acts sometimes also contain rules about the use and length of storage of specific criminal data, e.g. the use and storage of data as a result of the interception of telecommunications or other intrusive investigation methods that might lead to an indiscriminate amount of personal data.

The dividing line between data protection, criminal procedure and rules organising the police, is not the same in all countries. The rules of criminal procedure differ widely between the countries while remaining within the framework of the Human Rights Convention. The level and nature of crime in member countries differ, as do their policies in criminal matters. The varying pressing social needs in the countries differ and have their legitimate influence on the regulation of police powers. It is not the task of the CJ-PD to make proposals with regard to rules of criminal procedure. This does not affect the fact that the CJ-PD is competent for the application of data protection principles in Codes of Criminal Procedure. It is neither possible nor desirable, though, to strive for a far-going harmonisation of data protection rules for criminal data. This does not affect the fact that, from a data protection perspective, in view of the on-going development of information technology and its possible threats for private life, some questions may be raised to make national legislators in either area of law, aware of these threats so they can take them into consideration in any decision either to regulate or to abstain from regulation.

5. Criminal intelligence

5.1. Scope of the concept of 'criminal intelligence'

A new phenomenon that is not specifically dealt with in Recommendation No. R (87) 15 is the area of criminal intelligence. This term is not unambiguous. Several distinctions can be made.

a. Hard data versus soft data. The police data about criminals may vary from (1) data flowing from a well established source to (2) data based on very vague indications about somebody's possible involvement with serious crime. The first category is referred to as hard data, the second as soft data. This last category may even stem from an anonymous source, resulting in complete uncertainty about its trustworthiness. The nature of the information may yet be such that storage, at least for a limited period of time, might be deemed necessary for the proper performance of the police task.

b. Data about persons suspected of having committed a specific crime or about persons about whom there are indications that they are involved in committing or preparing a serious crime, either as part of an organisation or alone. As police and judicial powers in most national Codes of criminal procedure are limited to cases where there is a suspicion against a person with regard to a specific criminal offence, new information technology is increasingly used to store data about criminals as persons as such, without relation to specific criminal offences. The data can comprise both soft and hard data, as made explicit above. It does not necessarily meet the standard of a well established suspicion against a person, a standard which must be fulfilled in order to apply the powers conferred on the police in the Code of Criminal Procedure. Nevertheless many countries collect data which may even imply the profiling of the alleged criminal, his behaviour, his contacts and his way of life without much relevance with regard to a specific criminal offence. The data are used to solve any crime, either already committed or expected to be committed in the future. Their use is not limited to the investigation of, or use as evidence in, a specific criminal offence. As long as no specific rules are foreseen in a national Code of Criminal Procedure or a (regional) police law, general data protection principles apply to these data. The term 'criminal intelligence' will for the purposes of this paper further be used in this second sense.

This implies that data are not regarded as 'criminal intelligence' if they are gathered in the course of a criminal investigation where there are reasonable grounds for a suspicion against an individual person having committed a specific criminal offence, irrespective of whether:

(1) these data are only used in the criminal case in the investigation of which they were gathered or are afterwards also used to possibly solve future crimes as well;

(2) these data have been gathered using powers granted in the Code of Criminal procedure or not.
In some countries the data cannot be used as evidence in a trial. They serve only to guide the police investigations. They might become relevant, though, during a trial if the defence challenges the way the evidence has been gathered. The legality of their storage might then be questioned since the evidence might be a fruit of the poisoned tree.

5.2. Questions with regard to criminal intelligence

There are different questions to be answered with regard to the collection and storage of criminal intelligence.

5.2.1. Who can be data-subject as part of criminal intelligence?

Since the right to respect for private life implies that not everybody can indiscriminately become the subject of criminal intelligence, the law must define the criteria for identifying the targets that can be the subject of criminal intelligence. These criteria will differ according to national law and can be criteria based on content or on procedure. Criteria based on content are, for example, the restriction to gather criminal intelligence only in cases of serious organised crime and crimes of a comparable threat to society. A criterion based on procedure is for instance that a Ministry of Justice, a Ministry of Internal Affairs, a judge or a public prosecutor, mandating the collection of criminal intelligence during a limited period of time and, if possible, within a geographically defined area about a precisely defined group of persons who are suspected of being involved or becoming involved in a specifically circumscribed area of crime. The question then to be answered is whether the mandate should be a publicly available document, either from the very beginning, or as soon as possible if the investigation can no longer be jeopardised.

5.2.2. Storage of data about persons related to targets of criminal intelligence

The principle is that data are processed relating to criminal offences about a group of persons, to be precisely defined by law, with regard to whom there is not yet any concrete suspicion on reasonable grounds of committing a specific offence. When these persons are profiled with regard to their behaviour, as far as that might be criminally relevant, it is necessary to store data about other, unsuspected persons, as well, even though they do not fit the criteria of targets of criminal intelligence. Two categories can be distinguished.

(1) persons with whom targets of criminal intelligence are in contact either physically as observed in the ordinary world or by telecommunications as observed by means of electronic surveillance of their telecom (telephone, fax, electronic mail etc), or

(2) persons who inform the police (informants, often criminals themselves): a record of all their conversations with the police and, moreover, perhaps of their own behaviour, in order to establish their trustworthiness and to keep control over the policemen that maintain the contact with informants.

The data about the persons under (1) and (2) should be kept separate from the data about the targets of criminal intelligence as they are collected for different purposes. The data under (1) should be restricted to the extent that is necessary to get a clear picture of the data-subject. The purpose of storage does not allow a profiling of these contacts themselves. The data under (2) could therefore be more extensive in order to allow in court, if contested, to judge the legality of the gathering of data (and therefore the admissibility of evidence) gathered from these informants. This can imply that the data gathered about persons under (2) are more extensive than about persons under (1), since the data are gathered for different purposes.

The different purposes also imply that decisions about queries, matching and datamining should be justified against the background of each separate set of data, taking account of the purpose for which they are processed. The purpose of the data under (1): they are meant to give information about the target of the criminal intelligence; under (2): to check the trustworthiness of the informant. Other usage of these data should be compatible with these original purposes if the use is not restricted to these purposes only. The processing by matching, combining and datamining of the data under (1) and (2), in order to find patterns of contact between criminals and establish new suspects or new targets of criminal intelligence, can be regarded as a form of compatible use. This is less evident where these data are used outside the police task, e.g. to establish somebody's

trustworthiness to fulfil a specific task outside the police. In view of article 9 of Convention 108, such use would need an explicit legal basis.

5.2.3. How long should criminal intelligence data be stored?

The law should be explicit about the duration of storage of criminal intelligence. As a direction of thought, one could think of a period of some years after the last time any relevant data has been added to the record. After this period one could think of a periodic review (as is done in article 112 of the Schengen Agreement). If, after a review, there are no reasonable grounds to justify further storage then deletion should be the rule. Data protection does not justify storage simply for the reason that you never know whether any data 'might perhaps come in handy in any unforeseeable future'. This leaves open the possibility that each review leads to the decision to continue storage, in the end possibly for an indefinite time. If there are good reasons to do so each time, this must be accepted. One could also think of a stricter system of obligatory deletion after a certain lapse of time.

5.2.4. Final remark on criminal intelligence

Any regulation of criminal intelligence only makes sense if the storage and use of criminal data about other unsuspected persons is not allowed unless for specific purposes and for short periods mentioned in the law.

Proposal: It is recommended that member States define in their domestic legislation, in a strict sense, the targets that can be subject of criminal intelligence. A time-limit for periodic review of continued storage should be made explicit in the law.

6. The data collected by the police during an individual criminal investigation

6.1. Scope of the problem

The rapid changes in information technology do not leave the police unaffected. The instruments of information technology make work more effective, both for criminals and for the police. Sometimes this means that the police, in order to do their work properly, have to collect vast amounts of data either by downloading computers during searches in premises, by intercepting (tele)communications or by searching the E-mail of criminals. Particularly criminals participating in organised crime may engage in massive storage and exchange of data in order to run their organisation. The data is sometimes collected by rather intrusive investigational methods granted to the police under the Code of Criminal Procedure. They often contain personal data in bulk, possibly completely unrelated to the crime under investigation or any other crime, but entered nevertheless into the police computers in the course of a criminal investigation. 'Unrelated' is meant in the sense that no grounds for the specific criminal investigation at hand justify the continued storage and use in the light of article 8. The storage can be justified only for the time needed to find out that they are really unrelated, unless other compatible use or other use explicitly permitted by law come in view.

6.2. Other use

To what extent are the police entitled to use this data also in other criminal investigations? What do the principles of purpose specificity and compatibility mean within this context? What are the limits of article 9 of Convention 108 to allow by law other purpose to be served by the data?

It is arguable that the data can be used to investigate new unrelated offences if it is clear from the collected data - this means: without comparing or matching with data collected in other cases - that there are enough indications to base a reasonable suspicion for this new offence. The police are obliged to notify any criminal offence they have knowledge of. It is irrelevant whether this knowledge is the result of the use of investigative powers in another, even completely unrelated case. This sort of use can therefore be regarded as compatible with the original purpose.

The next question is whether it can be used for the investigation of other related or, even more broadly, for similar offences, also in cases where from the data no reasonable suspicion can be inferred. According to some legal systems, in some cases: yes.

1. In cases where data about a suspect or even a person condemned afterwards is collected in the course of one investigation, the data about him is stored with the purpose of further usage. E.g. fingerprints and photographs, besides the nature of the offence, remain available for the solution of possible future offences. This may be regarded as compatible use. There is divergence between member States as to the necessity of deleting such data in cases of acquittal by lack of evidence though the suspicion remains. It is less questionable that these data should in principle be deleted in a case where somebody's innocence has been established or where afterwards any suspicion has been removed.

2. Data about persons other than the suspect or the convicted person collected in the course of a criminal investigation are, in principle, collected for that investigation. A use for other purposes, e.g. for a possible investigation of future criminal offences, cannot be regarded as compatible with the original use. Thus, if such use is deemed necessary, a legal basis in the sense of article 9 of Convention 108 is needed. One could think of cases where such data are used to update files about targets of criminal intelligence.

Domestic law should give explicit answers to these questions. Convention 108 seems to leave room for some digression.

6.3. Final remark

From a practical point of view, one could think of data collected in the course of a specific criminal investigation being used by the police indiscriminately in order to see whether perhaps there might be something useful in it, e.g. to solve yet unresolved criminal cases. This could however easily lead to a general power of the police to survey large portions of the population on the basis of any data once legitimately gathered during the course of a criminal investigation. If however one departs from the principle 'if there is no crime, there is no investigation', it might be questioned whether such broad use would fit the compatibility test of article 8, under b, of Convention 108. In the Campbell-case the European Court of Human Rights judged that 'the existence of facts or information (should) satisfy an objective observer' that there is reasonable cause to use such data for the purpose of combating crime (1992, 15 EHRR 137). Since the processing of criminal data, being sensitive data, could be regarded as an interference with private life, such cases need to be legitimised in the sense of paragraph 2 of article 5 of the Convention on Human Rights.
This leaves unaffected the matching, datamining and other forms of processing of personal data, if allowed by law, with regard to any existing file, whether public or established for a certain legitimate purpose and therefore restricted in its use.
Proposal: It is recommended that any power to perform a general data surveillance check or matching for the purposes of the suppression of crime on the basis of police data gathered in the course of criminal investigations on the basis of vast amounts of persons possibly completely

unrelated to any crime, be limited to specific cases described in the Code of Criminal Procedure and be granted on the basis of a specific mandate of the judiciary.

7. Datamining with other data than police data

Computing power has increased enormously. It has become possible to interconnect and compare extensive databases in order to find evidence about crime also about persons that might be completely unsuspected beforehand. In most Codes of Criminal Procedure there are powers for the judiciary to request the submission of any objects, including data carriers or data unrelated to its carrier. Most of these powers were formulated in an age where there was no practical reason to distinguish between information about one person and information about a vast amount of people. Since information technology has made the searching, the monitoring of communications and the combining of data so easy, it might be argued that from a perspective of data protection this distinction has gradually become legally relevant. It is therefore recommended that this differentiation in a Code of Criminal Procedure be made explicitly wherever it might be relevant. The submission of a vast amount of personal data in bulk for purposes of criminal investigation should be made dependent upon stricter criteria and the interpretation of these criteria in a specific case be made dependent on the decision of a more independent (judiciary) authority than the submission of data about some individual person or persons, whose identity is specified before the search is done and their data are submitted. Several situations can be distinguished.

(A) A rather recent development made possible by information technology is the collection of large amounts of personal data from open sources. From this point of view Internet and digitalized public files should be dealt with specifically.

1. The Internet allows collection of data about persons. Like everybody else, the police, if acting in the legitimate performance of their task, can consult the open sources on Internet, as well as sources from abroad. No specific power laid down in domestic legislation is needed, as these forms of consultation do not constitute an invasion into private life. Personal data about subjects that are already investigated for the purposes of a criminal investigation can thus be collected and added to the police data if they might be or become relevant for the case. This should be distinguished from the indiscriminate collection about a vast amount of persons previously unknown to the police. As everybody can perform these forms of collection, one could argue that this is not denied to the police if this is necessary for the performance of their task. A legally relevant borderline is passed though if such massive collection is matched with police files. A general matching of downloads from Internet with police files, just in order to see whether perhaps a criminal offence can be detected, could easily imply a general surveillance of large parts of the population to the extent that there is an invasion of private life without sufficient legitimate grounds. This leaves it to member States to regulate such matching specifically linked to the investigation of a specific criminal offence.

2. All countries have public files containing all sorts of personal data that can be consulted by anybody for a wide range of different purposes, e.g. the land estate register or the commercial register containing the personal data of persons involved in the management of a company. Until a few years ago it was not possible to combine these files and make queries in order to discover hitherto unknown relations. Since some of these public files become available digitally on CD-ROM or on Internet, extensive queries, according to all sorts of criteria, combining different public files, have become possible, unless specific technical measures have been taken to prevent such queries. Legislators have established a public file with the often implicit idea that some specified information about individual persons can be consulted. It is not self-evident that this implies automatically that these files can also be made digitally accessible with the result that on the basis

of the information in the file individual persons, hitherto unknown, can be found. It seems that from a data protection point of view security devices are needed to prevent the public file from being compared with other (public) files in an unlimited way. For example, a group of previously unknown persons that fulfils a predetermined set of characteristics can be identified, contrary to any purpose of any of the public files involved. Different concepts, all referring to some slightly different characteristics, have become the vogue: datamining, matching, knowledge discovery, information resource management etc.

This immediately raises the question of whether the police are allowed to compare these files mutually or with police files, for example in order to enrich these files or to detect new crimes. Again, it is proposed limiting these forms of matching to specific cases of an investigation of a criminal offence on the mandate of the judiciary, thus excluding general surveillance by the police of large portions of the population outside the situation of the investigation of a specific criminal offence. Datamining with regard to public files, or the matching of different public files, if deemed necessary in order to detect crime, should be explicitly authorised by law according to specific criteria.

(B) On the basis of article 6 of the EC Directive of 10 June 1991 (91/308/EEC) on prevention of the use of the financial system for the purpose of money laundering, there is general collection of certain data about unusual transactions for the purpose of preventing criminal offences. These data are collected for the purpose of the suppression of a specific category of crime, though about unsuspected persons, who do not fulfil the criteria of being subjects of criminal intelligence. According to this article, in principle these data may not be used for other purposes, unless explicitly permitted by law. For a specific area there is thus general data surveillance of the population for the purpose of the suppression of a specific form of crime according to specific criteria. The question to be answered explicitly by the legislator is whether, and if so to what extent, the police have access to the data thus gathered. It seems desirable that the police have at least access to the financial data thus collected about the persons already legitimately in their own files. It is less evident that these data may be indiscriminately used by the police, unless there is an explicit legal base according to certain procedures.

Proposal: It is recommended that the Code of Criminal Procedure allow for a mandate of the judiciary in specific cases if this is deemed necessary for the investigation or the ending of a specific criminal offence to match public files, financial data about unusual transactions or a download from Internet with police files.

8. Genetic data

Scientific progress in the use of DNA as a means of recognising people will increasingly lead to the importance of this tool. For that purpose many countries have or are developing DNA bases. Within the EU a transnational database is being discussed. From a data protection point of view, the following can be brought forward.

DNA is scrutinised for a number of reasons. Some persons are convicted because their DNA has been found at the place of the crime. The DNA is part of the evidence that the person is guilty. In case of sexual offenders, these data are stored and used in the investigation of future crimes. The legislator should be explicit about whether to limit the use of DNA of sexual offences, or to extend the use of the DNA bank also to petty offences, such as simple maltreatment. If the use of a DNA bank by law is limited to sexual offences, DNA found at the place of a petty offence can be used to identify the perpetrator. It is however excluded that the DNA will be used again in the future if any DNA is found.

DNA is used to identify perpetrators of serious criminal offences. It can also happen that the DNA test leads to somebody's acquittal. The test can prove that he did not commit the offence. If a DNA test has proven that somebody is not guilty of a criminal offence (or more limited: a sexual offence), storage of the data in the DNA bank for the purpose of investigating possible future crimes should be forbidden.

In practice, it cannot be excluded that DNA of one person can be used to identify another person in the same genetic line. The legal question then arises, of whether this is permitted. E.g. the DNA bank contains DNA of a father, and his fugitive son is suspected of having committed a sexual offence, having left traces of DNA, but the DNA of the son is not available. Can the DNA of the father be used as evidence that the son has committed the crime? The legislator has to answer the question whether, from a legal point of view, there is a good reason why somebody whose father appears in the DNA bank should be an easier target for law enforcement than somebody whose relatives have not been caught by the police. One could think of limiting such use to exceptional, serious cases.

Sometimes large parts of the population are requested to co-operate for the solution of some criminal offences by making available their DNA (or other biometric data, such as fingerprints). On a voluntary basis this is possible. Other use of these data, e.g. for the solution of other criminal offences without additional consent for this other use, must be regarded as incompatible with the original purpose. This implies the deletion of the data after the investigation of the criminal offence in question has been ended.

Proposal: A multidisciplinary group within the Council of Europe will study certain problems in relation to genetic data. The group could take the questions mentioned above into account.

9. Notification

In principle, persons should be informed about the data that is collected about them, in order to enable them to seek an effective remedy against any alleged invasion of their private life (cf. article 13 ECHR). Suspects ought to be informed as soon as they are arrested of the nature and the cause of the accusation (cf. article 6 ECHR). In a hearing they will be confronted with the collected evidence. In a criminal investigation other data subjects than the suspect might become involved as well. The Klass-case of the European Court of Human Rights of 6 September 1978 (Series A, nr 28) allows for the postponement of informing the data subject as long as this is necessary in order not to jeopardise the performance of the police task. In case of criminal intelligence this exception will probably be applicable in nearly all cases.

The question arises of the extent to which persons concerned should be informed in cases of large downloads of personal data from computer systems during a search. The search as such can no longer be jeopardised, so the Klass-criterion does not apply. An exemption to the obligation to notify will in some cases be possible on the basis of a disproportionate effort. However, if persons exert their right of access with regard to the police, they will have to be informed that data about them have been collected during a search. Moreover data subjects can be informed by the system keeper of the downloaded computer. In principle, he does not have any obligation to confidentiality about the data the police downloaded from his computer. If it is deemed to be necessary that specific categories of controllers of data files remain silent towards the data subjects about the data that the police have collected from them, this should be explicitly provided for by law. One could think of special circumstances where telecom operators or bankers, having submitted data to the police, could be obliged by law to keep this fact secret from their clients. The legislator could

impose such an obligation on Internet Service Providers in cases of the investigation of electronic mail. A general duty of private persons to remain silent towards data subjects if personal data have been submitted or seized by the police must probably be regarded as a disproportionate measure.

This situation should be distinguished from the case where personal data are monitored and collected during a certain period of time on the basis of a legal mandate, e.g. the collection of traffic data in telecommunications in the future. The investigative power would be jeopardised if the data subjects that are monitored are informed beforehand. These are secretive investigative powers by their nature so the data-subject can only be informed afterwards. In these cases it can be useful if the legislator in a general sense obliges private persons on whose co-operation the police depend, to remain secret towards the data-subject at least during the period of the monitoring. After the monitoring data subjects should in principle be informed about the collection of their personal data, e.g. if their telephone conversations have been intercepted during a call with a target of an interception mandate. If this information is omitted for reasons of disproportionate effort, a possible request in the exertion of the right of access by the data subject has to be granted, unless proper performance of the police task would be jeopardised.

Proposal: It is recommended that the legislator be explicit about the circumstances under which the data subject has to be informed, either on the initiative of the police, or upon request of the data-subject. The position of private parties co-operating with the police in submitting personal data about third persons should be made clear.

10. Transborder data flows

Data collected and stored legally by the police can also be transmitted to police bodies of other countries under point 5.4 of Recommendation No. (87) 15 regulating the use of personal data in the police sector. This can be refused if there are specific rules because of the sensitiveness of criminal data or some categories of criminal data (e.g. criminal intelligence) and the other country does not have an equivalent level of protection (article 12 of Convention 108).

The communication should be to police bodies in the other country. This means that the police bodies of the receiving State, according to its domestic law, may communicate these data to government bodies for administrative purposes. This is only different if the country of origin stipulates explicitly that the data are communicated for police purposes only. Such a stipulation is, however, only effective as long as the police bodies in the receiving country do not have a legal obligation under their domestic law to communicate their data to other bodies. Receiving States should inform States of origin about such legal obligations.

The Schengen Agreement and Europol have their own data protection regime that is adequate. There seems to be no specific need to develop new instruments specific to transborder data flows of police data besides the elements already mentioned for national law, which can not avoid having their effect at the international level as well.

11. Accountability

Data protection and the effective performance of the police task are sometimes hard to reconcile. It is accepted that the police for the purpose of preventing or investigating crime need vast amounts of personal data. However, the processing of these data cannot be unlimited and should be regulated by law. In order to allow the competent authorities to legislate in a timely fashion, either to grant the police extra powers to fulfil their task, or to protect citizens against unjustified intrusions into their private lives, one could think of instruments to allow the authorities to monitor developments in this

field. One of these instruments could be the obligation for the police to report about the quantity and the precise ways certain powers granted them by law are exerted with regard to the processing of personal data. E.g. one could think of an obligation to report the number of persons subject to criminal intelligence. The question is left unanswered whether this should be a secret report to the government or a public document allowing parliament to control the use of powers that might affect private life.

Proposal: National legislators should consider the possibility of regulatory instruments to monitor the use of investigative methods of the police involving the collection, storage and use of personal data.

12. Supervisory authority

The countries that have implemented the EU data protection directive 95/46/EEC did not make any substantial exception on the powers of the independent supervisory authority with regard to the police, although the directive is not applicable to police files as such. In general terms an improvement in supervision and law enforcement of data protection rules with regard to the police may therefore be expected. It is recommended that other member States of the Council of Europe establish a similar regime of supervision for police files in their countries. This would be advantageous to the unhampered international exchange between police bodies in combating international organised crime.

Proposal: Member States should establish in domestic law a system of independent supervision over police files in their countries with effective powers to enforce data protection rules in case of non-compliance.

13. Conclusion

It is proposed that the Committee of Ministers of the Council of Europe change their original decision to evaluate the 1987 Recommendation periodically in the sense that periodically the question be answered whether any additional international instrument should be developed.
The Committee could further give guidance to legislators in the Member States with regard to at least the following questions. These could be further elaborated in close co-operation with the CD-PC since the borderline between data protection, criminal procedure and police law will not be the same in all countries and many questions touch all these areas of law.

Proposals:

1. National legislators should explicitly answer a number of questions of data protection, either in the national Data Protection Act, the national Code of Criminal Procedure or the Police law.

2. Member States should define in their domestic legislation, in a strict sense, the targets that can be the subject of criminal intelligence. As a direction of thought, one could think of serious organised crime and crimes of a comparable threat to society. A time limit for periodic review of continued storage should be made explicit in the law.

3. Any power to perform general data surveillance checks or matching for the purposes of the suppression of crime on the basis of police data gathered in the course of criminal investigations on the basis of vast amounts of persons possibly completely unrelated to any crime should be limited to specific serious cases described in the Code of Criminal Procedure and be granted on the basis of a specific mandate of the judiciary.

4. The Code or Criminal Procedure should make clear in what cases police files may be matched with public files, financial data about unusual transactions or a download from Internet.

5. The law should be explicit about the circumstances under which the data subject has to be informed, either on the initiative of the police, or upon request of the data subject. The position of private parties co-operating with the police in submitting personal data about third persons should be made clear.

6. Member States should establish in their domestic law a system of independent supervision over police files in their country with effective powers to enforce data protection rules in case of non-compliance.

7. It is recommended that any power to perform a general data surveillance check or matching for the purposes of the suppression of crime on the basis of police data gathered in the course of criminal investigations on the basis of vast amounts of persons possibly completely unrelated to any crime, be limited to specific cases described in the Code of Criminal Procedure and be granted on the basis of a specific mandate of the judiciary.

8. It is recommended that the Code or Criminal Procedure allows for a mandate of the judiciary in specific cases if this is deemed necessary for the investigation or the ending of a specific criminal offence to match public files, financial data about unusual transactions or a download from Internet with police files.

9. A multidisciplinary group within the Council of Europe will study certain problems in relation to genetic data. The group could take the questions mentioned above into account.

10. National legislators should consider the possibility of regulating instruments to monitor the use of investigative methods of the police involving the collection, storage and use of personal data.

APPENDIX B

Text of Recommendation 1181 (1992) of the Parliamentary Assembly

RECOMMENDATION 1181 (1992)[1] on police co-operation and protection of personal data in the police sector.

1. As a result of the Schengen Agreement, the European States co-operating in that agreement will proceed with the exchange of automatically processed personal data in the police sector. It is most likely that such an exchange will cover the whole of the European Community after the disappearance of frontier controls at its internal borders.

2. Nowadays there is already an intensive exchange of data in the police sector among Council of Europe member States on a bilateral or multilateral basis and through Interpol.

3. It is of vital importance for an efficient combat against international crime that it is fought at national and at European level.

4. An efficient fight against crime implies an exchange of data in the police sector.

5. In this respect it is useful to recall the Assembly's Recommendation 1044 (1986) on international crime and its plea for a European information and intelligence centre (Europol), and Recommendation No. R (87) 15 of the Committee of Ministers to member States of the Council of Europe regulating the use of personal data in the police sector.

6. It is necessary, however, that there be adequate protection of personal data in the police sector and one may note with satisfaction that the Council of Europe concluded, in 1981, a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. However, in order to be fully effective, it is not sufficient that this convention has, to date, only been ratified by eleven member States.

7. The Assembly therefore recommends that the Committee of Ministers :

i. draw up a convention enshrining the principles laid down in its Recommendation No. R (87) 15 ;

ii. promote the application of these principles in the exchange of data in the police sector between member States and between member States and third countries via Interpol. In this respect the implementation of the following principles is of the utmost importance :

a. data should be accurate, relevant, not exceed the purpose for which they are stored and, where necessary, kept up to date ;
b. they should be screened before they are stored ;
c. an individual should have the right to know whether personal data concerning him are kept ;
d. he should have an appropriate right of access to such data ;
e. he should have the right to challenge such data and, if necessary, have them rectified or erased ;

[1] Text adopted by the Standing Committee, acting on behalf of the Assembly, on 11 March 1992. See Doc. 6557, report of the Committee on Legal Affairs and Human Rights, Rapporteur : Mr Stoffelen

f. individuals who are denied access to files relating to them should have a right to appeal to an independent authority which has full access to all relevant files and which can and should weigh the conflicting interests involved ;
g. there should be an independent authority outside the police sector responsible for ensuring respect of the principles laid down in such a convention ;

iii. appeal to member States to ensure that data in the police sector may only be exchanged with other member States and with Interpol on the lines provided for in the proposed draft convention.

Decision No. CM/537/220692 of the 478th meeting of the Committee of Ministers
June 1992

DECISION No. CM/537/220692

Ad hoc terms of reference

1.	Name of the Committee:	PROJECT GROUP ON DATA PROTECTION (CJ-PD)
2.	Source of terms of reference:	Committee of Ministers
3.	Completion date:	25 September 1992
4.	Terms of reference:	
	To give an opinion on Assembly Recommendation 1181 on police co-operation and protection of personal data in the police sector	
5.	Other Committee to be informed of terms of reference:	Steering Committee on Legal Co-operation (CDCJ)

Decision No. CM/547/180193 of the 486th meeting of the Committee of Ministers
January 1993

DECISION No. CM/547/180193

Ad hoc terms of reference

1.	Name of the Committee:	PROJECT GROUP ON DATA PROTECTION (CJ-PD)
2.	Source of terms of reference:	Committee of Ministers
3.	Completion date:	December 1994
4.	Terms of reference:	

To evaluate the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector and, in particular the need to revise the text, namely its scope and principle 5.4 (international communication), bearing in mind the principles set out in Assembly Recommendation 1181 (1992).

5.	Other Committee to be informed of terms of reference:	Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD)

POLICE CO-OPERATION AND PROTECTION OF PERSONAL DATA IN THE POLICE SECTOR
Recommendation 1181 (1992) of the Parliamentary Assembly
(CM/Del/Dec(93)486/19, CM(95)1, Appendix III)

Decision

The Deputies adopted the following supplementary reply to Parliamentary Assembly Recommendation 1181 (1992) on police co-operation and protection of personal data in the police sector:

"1. The Committee of Ministers refers to its previous replies to Parliamentary Assembly Recommendation 1181 (1992) on police co-operation and protection of personal data in the police sector, adopted in June 1992 and January 1993 respectively. It wishes to remind the Parliamentary Assembly that, as indicated in its reply in January 1993, it instructed the Project Group on Data Protection (CJ-PD) to evaluate the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector, and in particular the need to revise the text, namely its scope and principle 5.4 (international communication).

2. The CJ-PD reached a number of conclusions which have been endorsed by the Committee of Ministers. The latter is therefore in a position to inform the Assembly that, in its opinion, Recommendation No. R (87) 15 gives adequate protection for personal data used for police purposes and that, at this state, there is no need to revise it, or parts of it. Principle 5.4 of Recommendation No. R (87) 15, especially when read together with paragraphs 56 to 80 of its Explanatory Memorandum, appears flexible enough to meet the present and foreseeable requirements of international agreements on the exchange of data for police purposes.

3. However, bearing in mind inter alia the implementation of new systems for the sharing of personal data used in the police sector, such as EUROPOL, the rapid development of new technologies and the concerns expressed by the Parliamentary Assembly, the Committee of Ministers considers that the relevance of Recommendation No. R (87) 15 should be reviewed on a regular basis. It has therefore decided that the next review will be carried out in December 1998 and thereafter on a four-yearly basis."

Report on the third evaluation of Recommendation N° R (87) 15 regulating the use of personal data in the police sector, done in 2002

INTRODUCTION

1. By Decision No. CM/537/220692 adopted in June 1992, the Committee of Ministers instructed the Project Group on Data Protection (CJ-PD) to give an opinion on Assembly Recommendation 1181 (1992) on police co-operation and protection of personal data in the police sector. In January 1993, by Decision No. CM/547/180193, the Committee of Ministers instructed the CJ-PD "to evaluate the relevance of Recommendation No. R (87)15 regulating the use of personal data in the police sector and, in particular the need to revise the text, namely its scope and Principle 5.4 (international communication), bearing in mind the principle set out in Assembly Recommendation 1181 (1992)". Furthermore, by a decision adopted on 7 February 1995, the Committee of Ministers considered "that the relevance of Recommendation No. R (87)15 regulating the use of personal data in the police sector should be reviewed on a regular basis. It has therefore decided that the next review will be carried out in December 1998 and thereafter on a four-yearly basis". In accordance with the above-mentioned terms of reference two evaluation reports were prepared in 1994 and 1998.

2. According to the terms of reference of the CJ-PD ("*prepare the evaluation of Recommendation No. R (87) 15 on the use of personal data in the police sector, which shall be transmitted to the Committee of Ministers by 2002, at its request and through the CDCJ")* the third evaluation report will be submitted, through the European Committee on Legal Co-operation (CDCJ), to the Committee of Ministers in 2002. Taking into account the close links between the tasks of its Working Party on data protection and police and judicial data in criminal matters (CJ-PD/GT-PJ) and the content of Recommendation No. R (87) 15, the CJ-PD decided to entrust its Working Party with the preparation of a draft report on the third evaluation of this Recommendation. This draft report was submitted to the CJ-PD for revision and approval at its 40th plenary meeting from 7 to 9 October 2002.

3. When preparing the report on the third evaluation of Recommendation No. R (87) 15, account was taken of: the previous two evaluations; the Regional Seminar on "Data Protection in the Police Sector" organized by the Council of Europe in 1999 in the framework of its "Activities for the Development and Consolidation of Democratic Stability" (ADACS) and as a contribution to the Stability Pact for South-East Europe; the results of the Project "Fight Against Crime and Personal Data Protection" (FALCONE Programme) which was launched on the initiative of the Italian and Portuguese Data Protection Commissions and approved and sponsored by the Commission of the European Communities; and developments since the last evaluation, in particular the case law of the European Court of Human Rights in this matter.

4. In accordance with the above-mentioned instructions and bearing in mind the above-mentioned documents and activities, the report on the third evaluation of Recommendation No. R (87) 15 regulating the use of personal data in the police sector was prepared. In order to prepare this third evaluation report, the CJ-PD examined Recommendation No. R (87) 15 and agreed that its principles are still relevant and therefore considered that it is not necessary to revise them at present. Furthermore, the CJ-PD pointed out that this Recommendation is referred to in other international instruments such as the Schengen Agreement and the Europol Convention. Therefore, the CJ-PD does not recommend any revision of Recommendation No. R (87) 15 or the preparation of a new recommendation in the police field. However, the CJ-PD noted that since the last evaluation in 1998, there have been new developments in this field which deserve examination. The CJ-PD agreed that

these new developments could be addressed by a teleological interpretation of the existing Recommendation.

5. The CJ-PD revised and adopted the report on the third evaluation of Recommendation No. R (87) 15 regulating the use of personal data in the police sector during its 40th plenary meeting from 7 to 9 October 2002. The CJ-PD submitted this report to the CDCJ requesting that it transmit the report on the third evaluation to the Committee of Ministers in 2002.

6. Taking into account the multidisciplinary composition[1] of the Working Party (CJ-PD/GT-PJ) which prepared the first draft report on the third evaluation, the conclusion reached during the second evaluation of Recommendation No. R (87) 15 ("[..] give guidance to legislators in the member States […]. These [questions] could be further prepared in close co-operation with the CDPC since the borderline between data protection, criminal procedure and police law will not be the same in all countries and many questions touch all these areas of law"] as well as the issues concerned (police and judicial data in criminal matters), the CJ-PD suggested that the CDCJ send the final version of this report, for information, to the European Committee on Crime Problems (CDPC) and, subject to the agreement of the CDPC, to its relevant subordinate committees, in particular the Committee of Experts on Police Ethics and Problems of Policing (PC-PO) and the Committee of Experts on the Operation of European Conventions in the Penal Field (PC-OC).

REPORT

a) Distinctions between judicial and police data

7. Under criminal procedure, the same personal data may be processed, at the same time, even in identical documents, by the police and the judicial authorities. Telephone tapping provides an illustration of the mixed nature of some data: a judge may authorise telephone tapping but the data are then collected by the police before the data are transferred again to a judicial authority. In these cases there is the risk of a grey area where some police data go to a judicial sector and some judicial data remain in the police sector. This can give rise to confusion in qualifying data as judicial or police data. This must not be used as a loophole for not applying the data protection principles in these sectors, or for avoiding determining who is controller of the file or the degrees of responsibility for each processing operation. It is however clear that each level of authority must respect its own rules.

---

[1] The following four experts were appointed by the CJ-PD:

- Mr Marc BUNTSCHU, Switzerland (Deputy Head of the Secretariat of the Swiss Data Protection Officer)

- Mr Giovanni BUTTARELLI, Italy (Secretary General of the *Garante per la Protezione dei Dati Personali*)

- Mr Alexander PATIJN, Netherlands (Legal Adviser at the Ministry of Justice)

- Ms Kinga SZURDAY, Hungary (Senior Legal Counsellor at the Ministry of Justice).

In accordance with the terms of reference from the CJ-PD, the European Committee on Crime Problems (CDPC) and its relevant subordinate committees could also participate in the composition of the CJ-PD/GT-PJ. Therefore, the other three experts of the CJ-PD/GT-PJ were appointed by the following committees:

- The European Committee on Crime Problems (CDPC) appointed Mr Hughes BRULIN, Belgium (Deputy Legal Adviser, Directorate General on Penal and Human Rights Legislation, Ministry of Justice).

- The Committee of Experts on Police Ethics and Problems of Policing (PC-PO) appointed Ms Elenor GROTH, Sweden (Legal Adviser, Ministry of Justice)

- The Committee of Experts on the Operation of European Conventions in the Penal Field (PC-OC) appointed Mr Philippe BIJU-DUVAL, France (Bureau de Droit Pénal Européen et International, S.A.E.I., Ministry of Justice).

8. Criteria must be found to determine which specific rules are to be applied. To this end, in accordance with Article 2.d of Convention 108, the controller of the file "means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them". Therefore, national law should clearly determine whether the controller of the data file is the police or the judicial authority. Furthermore, the purpose of processing can also serve as a complementary criterion.

9. Taking into account the considerations above, the CJ-PD reached the following conclusion:

I. Distinctions between judicial and police data:
In order to make a distinction between judicial and police data, it would be advisable to make explicit who is the controller of the file in the sense of Article 2, paragraph 2, littera d. of Convention 108, with regard to judicial data and police data. The controller of the file in this sense need not necessarily be the same as the authority who, according to the code of criminal procedure, is responsible for making decisions on or conducting criminal investigations. Special care should be taken to avoid loopholes in responsibility, in particular when personal data are collected and used by the police following an order from the judiciary to use intrusive surveillance methods such as interception of telecommunications.

b) Types of files held by the police

10. In accordance with Paragraph 36 of the Explanatory Memorandum of Recommendation No. R(87)15, 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.

11. These police files are of various types depending on the purpose for which they have been set up. From a data protection point of view the qualification of the police files as belonging to one type or another type is very important because it will determine the type of control that will be exercised on the personal data contained in those files.

12. Principle 1.4 of Recommendation No. R (87) 15 states that "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."

13. The CJ-PD examined the various types of files held by the police and distinguished between "permanent files" and "ad hoc files" (these files are set up at the time of particular inquiries) in accordance with the terminology used in Recommendation No. R (87) 15. The CJ-PD agreed that the so-called "analysis files" in the Europol Convention, as well as the so called "temporary files " or "working files" in other contexts, are considered ad hoc files in the sense of principle 1. 4, 2nd paragraph of Recommendation No. R (87) 15.

14. The CJ-PD also agreed that both types of file –permanent and ad hoc- can contain so-called "criminal intelligence data" (also called "soft data" in some contexts) which are data that have not yet been verified and whose link with the police objectives must be prepared. These types of data, which give some unconfirmed indications or raise suspicions about the involvement of a person in one or several criminal offences, could present problems from a data protection point of view because they can be processed for different purposes or even for a general preventive purpose, even though it has not yet been established whether they are either adequate or accurate. An examination of these criminal intelligence data as a new phenomenon that is not specifically dealt with in Recommendation No. R (87) 15 was carried out in the report of the second evaluation of this Recommendation and some proposals were made (see document CJ-PD (2002) 01). The other type of data which are also contained in permanent and ad hoc files are the so-called "hard data", data which have already been verified. The main difference between these "hard data" and "criminal intelligence data" or "soft data" is their degree of accuracy or reliability (see in this respect Principle 2, paragraph 2 of Recommendation No. R (87)15).

15. From a data protection point of view, the control exercised over the permanent files is more strict, at least in terms of notification, communication and storage, than that exercised over ad hoc files. Nevertheless, the non-permanent character of these ad hoc files could prompt the data protection authorities to control the quality of the data more frequently. In relation to ad hoc files, it should be borne in mind that, in accordance with Principle 1.4 of Recommendation No. R (87) 15, "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". Therefore, the CJ-PD examined these ad hoc files in detail.

16. The CJ-PD agreed that two types of ad hoc files can be distinguished:

- ad hoc files set up to solve a specific criminal offence that has already been committed;

- ad hoc files set up to gain knowledge of a specific criminal phenomenon such as an area in society about which there are indications that it is criminally affected. This type of files includes "analysis files", which are widely used to collect large amounts of data in order to gain knowledge about possibly criminal areas of society. As stated above, these files are not necessarily limited in time.

17. An ad hoc file to gain knowledge of a specific criminal phenomenon may only be set up if it is necessary for the prevention of a real danger in the sense of Principle 2.1 of Recommendation No. R (87) 15. These files may have a proactive function, in order to gather intelligence to prevent crime or to identify perpetrators. It might be necessary for the law to provide for specific procedural safeguards in order to ensure that the criterion of a real danger is fulfilled. The decision to set up the file could be confined to a certain authority and the principle of transparency in the sense of Article 8.a of Convention 108 should be taken into account. Derogation from the principle of transparency is only possible if the conditions of Article 9 of Convention 108 are fulfilled. The law could also provide for a procedure that obliges the monitoring of the continuing necessity of these sorts of ad hoc files, for example by the authority that decided on the establishment of the file.

18. In setting up such a file, the categories of persons and the categories of data collected about these persons should be specified in an exhaustive manner and in principle be made transparent. The data subject thus is able to establish whether he might be included in the file and, if so, what sorts of data

may be stored about him.[2] Some examples of this type of ad hoc files are the following: the investigation of a series of unresolved rapes during a certain period in a certain geographic area. Another example could be the fulfilment of police tasks in the case of a specific event, such as a football match or an important meeting of political leaders. Examples of ad hoc files of a more permanent character are files that are set up to gather criminal intelligence about lasting terrorist activities or specific forms of organised crime. Also the collection of data about hooligans in order to combat violence at any future football match (not only one) can be characterised as a more permanent ad hoc file.

19. Ad hoc files set up to gain knowledge of a specific criminal phenomenon ought to be distinguished from ad hoc files set up to investigate a specific criminal offence in order to allow the prosecution to bring the case before the court.

20. The exchange of data between different ad hoc files is only possible if there is a legitimate interest in the sense of Principle 5.1 of Recommendation R (87) 15. Within and between permanent files and within ad hoc files, indexes and search criteria may be applied in order to establish whether there is such a legitimate interest. Where an ad hoc file is set up to gain knowledge of a phenomenon of serious crime, linkage with other ad hoc files is more problematic as these files usually contain large amounts of data collected on the basis of more loosely formulated criteria. The seriousness of the criminal phenomenon that is targeted might, nevertheless, justify the application of an index-system between ad hoc files of this type in order to identify whether useful information is available in another unrelated ad hoc file set up for analysis purposes.

21. Ad hoc files that are set up to investigate a specific criminal offence might, however, contain an indiscriminate amount of data as these may be necessary to guarantee the suspect a fair trial. Possible evidence, including exculpatory evidence, cannot be deleted, even if it refers to third parties that are indirectly linked to the investigation of a criminal offence. The use of an index-system between ad hoc files of this second type can only be justified if a concrete link is apparent beforehand as a ground for its use. Such a concrete link can also be considered present if there are grounds for believing that by using an index-system to link different ad hoc files, such evidence can be produced or the accuracy of data can be checked. The index-system cannot, however, be used to undertake "fishing expeditions" in all the files for the investigation of whatever criminal offence. Arbitrary interferences with fundamental rights, especially of the private life, of third persons can thus be avoided.

22. The police may control personal data that have not yet been evaluated with regard to inclusion into a permanent or an ad hoc file. Examples are hard disks or address books that are seized during a search. Copies of hard disks, results of telephone intercepts or intercepted e-mails may also contain personal data that are completely irrelevant to any police or judicial purpose. These data should be kept or recorded separately until their evaluation and possible inclusion in a police file. Their use for other purposes can only be envisaged to counter an immediate and serious threat, e.g. a terrorist attack.

23. Taking the above considerations into account, the CJ-PD reached the following conclusions:

[2] Article 12.1 of the Europol Convention and Article 6 of the Council Act of 3 November 1998 adopting rules applicable to Europol analysis files (1999/C26/01) can be taken as examples for fulfilling these criteria.

II. Permanent files:
It would be advisable when setting up a permanent file to specify its purpose and the criteria for inclusion of personal data to the supervisory authority in order to enable the data subject to foresee whether his data may be included.

III. Ad hoc files for the investigation of specific criminal offences:
The collection of data for an ad hoc file set up for the investigation of a specific criminal offence is bound by the purpose of the file. This could lead to a file containing an indeterminate type of data, not least in order to avoid the risk of excluding exculpatory evidence. The indiscriminate use of such data, whatever the police purpose they are used for, could have the same effect as overall surveillance of the data subject and therefore could lead to an arbitrary interference in their rights and fundamental freedoms, in particular their right to privacy. The use of personal data contained in such an ad hoc file for the purposes of another ad hoc file set up for a specific inquiry could only be considered compatible with the original purpose for which the first file was set up when there is a concrete link between the two files or between the personal data contained in the files that justifies such use. Data, for example the results of a telecommunications intercept or the seizure of a hard disk, that are apparently irrelevant for the purpose should be deleted or returned.

IV. Ad hoc files for analysis of specific criminal phenomena:
It would be advisable that ad hoc files established for the purpose of analysis of a specific criminal phenomenon define the categories of persons about whom data may be stored and the categories of data about them with a certain degree of precision. In the case of serious criminal phenomena, it may be necessary to compare two such ad hoc files. Where, by comparison, concrete links are established, data from the first ad hoc file could be used also for the purposes of the second ad hoc file and vice versa.

V. Index systems:
Risks to rights and fundamental freedoms, in particular the right to privacy, which result from ad hoc files could be countered by compensatory substantive and procedural safeguards with regard to the use of the data. In particular, specific rules should regulate the use of an index system which enables access to data in the different ad hoc files. These rules should balance the obligation to protect the rights and fundamental freedoms, in particular the right to privacy with the necessity of using the data to combat crime effectively.

VI. Incompatible use:
The search for personal data in ad hoc files that cannot be regarded as a form of compatible use should be regulated in accordance with Article 9 of Convention 108 in the national code of criminal procedure or other laws.

c) The categories of persons about whom data may be stored

24. In the report of the second evaluation of Recommendation No. R (87)15 the following proposal was made "Member States should define in their domestic legislation, in a strict sense, the targets that can be the subject of criminal intelligence. As a direction of thought, one could think of serious organised crime and crimes of a comparable threat to society. A time limit for periodic review of continued storage should be made explicit in the law" (see document CJ-PD (2002) 01).

25. In accordance with Principle 2 of Recommendation No. R (87)15 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. Paragraph 2 of Article 8 of the European Convention on Human Rights states that any interference with the exercise of the right to respect for private life must be in accordance with the law and must be necessary in a democratic society in the interests, among others, of national security and for the prevention of disorder or crime. Therefore, according to the case law of the European Court of Human Rights, the storage of personal data for reasons of national security or in the interests of combating crime constitutes an infringement of private life and must have a legal basis that fulfils the conditions of Article 8, Paragraph 2 of the European Convention on Human Rights. The most explicit case is that of Rotaru v. Romania which states:

"The Court notes in this connection that section 8 of Law no. 14/1992 provides that information affecting national security may be gathered, recorded and archived in secret files.

No provision of domestic law, however, lays down any limits on the exercise of those powers. Thus, for instance, domestic law does not define the kind of information that may be recorded, the categories of people against whom surveillance measures such as gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed. Similarly, the Law does not lay down limits on the age of information held or the length of time for which it may be kept.

Section 45 empowers the RIS to take over for storage and use the archives that belonged to the former intelligence services operating on Romanian territory and allows inspection of RIS documents with the Director's consent.

The Court notes that this section contains no explicit, detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that may be made of the information thus obtained."[3]

26. This judgment is given with reference to national security, but in this respect is regarded to apply equally to police data gathered in ad hoc files for analysis of specific criminal phenomena. Similarly, it would be advisable to lay down the categories of persons about whom data may be collected and stored, the kind of information that may be recorded, etc.

27. In relation to the categories of persons about whom data may be stored in ad hoc or permanent police files, the CJ-PD pointed out that it would be advisable that these categories are laid down in law and they should be so precise that persons can reasonably foresee whether their data may be stored or not. The CJ-PD underlined that this categorisation applies to police files containing data that have been evaluated and found necessary for the purposes of the file by the police authorities and not to "raw" information. Among these categories of persons the following could be distinguished:

- persons where there are serious grounds for believing that they have committed or are about to commit a crime (suspects) ;
- persons convicted of having committed a criminal offence;
- victims of the criminal offence
- witnesses

[3] *Eur. Court HR, Rotaru v. Romania Judgment of 4 May 2000, Series A., paragraph 57.*

- third parties to the criminal offence. Persons who are indirectly linked to the investigation of criminal offences (contacts, informants, persons whose identity is revealed during the investigation, etc.) and who often have a direct or indirect relationship with the principal subjects of the investigation could be included in this category. This category comprises persons who are necessary for the investigation of the criminal offence but who cannot be included in any of the previous categories.

28. Taking the above considerations into account, the CJ-PD reached the following conclusions:

VII. The categories of persons about which data may be stored:
It would be advisable to specify with regard to ad hoc files for analysis of specific criminal phenomena the categories of persons about whom data may be collected and stored, as well as the kind of information that may be recorded. These categories should be defined with enough precision in order that individuals can reasonably foresee whether they fall under the scope of these categories or not.
Personal data about third parties should only be collected and stored when necessary for the purpose for which a file was set up.
It would be advisable to specify the categories of third parties whose data may be collected and stored because they have a certain relationship with the persons who are the principal subjects of the criminal investigation or because the collection of their data is necessary in order to meet the requirements of a fair trial.
It would be advisable to provide for a periodic review of the data stored in order to establish the adequacy of the category under which they are stored.

d) Length of storage and deletion of data

29. Principle 7 of Recommendation No. R (87) 15 states the following:

"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."

Taking the above-mentioned Principle into account, the CJ-PD examined the issue of the length of conservation of personal data processed by the police in the light of the developments which have occurred in the last years in relation to this issue.

30. With regard to duration of storage of data it was pointed out that the general rule is that if the data are no longer necessary for the purpose for which they were collected or for subsequent other purposes they should be deleted or archived.

31. The question of the conservation of data collected by the police, and in particular their deletion, should nevertheless be examined from the following points of view: the rehabilitation of convicted persons; unsolved cases (in some countries there is a time limit on how long a case remains open); the social reinsertion of convicted persons who have completed their sentences; and being able to recognise persistent offenders.

32. In this respect it was pointed out that the criminal record file is not a police file in all countries. Under Article 9 of Convention 108 on exceptions and restrictions, special procedures may be set up for consulting these files for appropriate purposes, e.g. the screening of persons for special functions. However, account should be taken of the provisions of the Council of Europe Recommendation No. R (84) 10 on the criminal record and rehabilitation of convicted persons.

33. The CJ-PD discussed the possibility of prescribing maximum lengths of time for the storage of data. When determining this period of storage, account should be taken of the prescription period of the specific criminal offence to which the data are related. The relevance of the data to the prevention of future criminal offences could – in the case of serious offences - be a criterion for the extension of the length of storage. The review procedure under the Schengen Agreement provides for deletion after one year unless the police can justify not deleting them. Recommendation No. R (87) 15 distinguishes between permanent files (which can be conserved for two or three decades) and ad hoc files for specific tasks such as political summit meetings, surveillance of specific organisations or public demonstrations (whose conservation must be justified once the event is over).

34. In relation to the soft data contained in permanent or ad hoc files, it would be advisable to require the establishment of mechanisms to update and control such data, for instance by periodic reviews every two to five years, in order to sufficiently ensure the quality and relevance of the data. After the purpose of the ad hoc files is fulfilled consideration should be given to whether they are to be deleted or whether they are to be transferred to the central data bank or the archives. The problem was raised of data which are collected and kept because “you never know” when the information may be useful. The notion of “real danger” in Article 2 of Recommendation No. R (87) 15 seems to preclude this.

35. A periodic review of the hard data should also be established in order to examine the adequacy of the quality of these data and to decide whether their storage is still necessary.

36. Taking the above considerations into account, the CJ-PD reached the following conclusion:

VIII. Length of storage and deletion of data:
The length of storage of personal data processed by the police should be established on the basis of the principle of necessity in relation to the purposes for which those data were stored.
In the case law of some national data protection supervisory authorities, "necessary" is strictly interpreted as something which is indispensable (in order to be collected, for instance). However, information which may be considered necessary at the time of its collection by a judicial authority may subsequently be found to be irrelevant in the light of developments in the inquiry. It would be advisable to fix maximum storage periods for the different categories of personal data processed by the police as far as possible, for the transparency of the legal system. Periodic reviews of the quality of personal data should be carried out in every case. When data are no longer necessary to fulfil the requirements of the police purposes for which they were collected, they should be deleted or be kept for the purposes of historical, scientific or statistical research. Their storage should be accompanied by safeguards and security measures to prevent their use for other purposes. In exceptional cases and in accordance with Article 9 of Convention 108, domestic law could lay down conditions for the re-use of these data for police purposes if these data are necessary for review procedures or for a concrete criminal investigation.

e) Screening of individuals

37. Principle 5.3. of Recommendation No. R (87) 15 states that "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. 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."

38. In relation to this principle, the screening of individuals was discussed[4], in view of their possible employment in sensitive posts, on the basis of data collected by the police. Principle 5.3.i of Recommendation No. R (87) 15 in principle excludes the communication of police data to private parties. Nevertheless, in some countries, with the data subject's consent, criminal convictions and police data are used as a basis for an opinion on the data subject's suitability for a certain, specified job. The opinion is given by an authority who is independent of both the data subject, applying for that job, and of the person deciding about the application. Police data may similarly play an important role in judging the trustworthiness of companies participating in public procurement.

f) Transfer of data to third countries which do not ensure an adequate level of protection

[4] Differing opinions were expressed in this respect: some experts thought that this text on the screening of individuals would be contrary to the content of Principle 5.3 of Recommendation No. R (87) 15 and therefore should be deleted; other experts thought that this question is a new problematic issue that should be dealt with in this evaluation and the text of this paragraph is not contrary to the above-mentioned principle of Recommendation No. R (87) 15.

39. The CJ-PD examined the issue of the transfer of data to third countries which do not ensure an adequate level of protection. This kind of transfer may lead to the infringement of rights and fundamental freedoms. Nevertheless, the purpose of fighting against serious crime may constitute a legitimate prevailing interest in the sense of the second indent of Article 2.2.a of the Additional Protocol to Convention 108. The transfer can be regarded to be justified if specific safeguards are provided for. Bilateral or multilateral agreements on the exchange of police data[5] may, for the purposes of data protection, contain provisions related to:

- the purpose for the use of the data;
- the types of data to be transferred;
- the authorities which could control the data;
- the prohibition in principle on the transfer of the data to other authorities or private parties;
- the obligation to ensure the right of the data subject to have information about his or her data and to obtain the correction of his or her data, as well as information about national law of the Parties restricting these rights;
- the obligation to delete the data after the fulfilment of the purpose for which the data were transferred and to inform each other about the time limit of storage of the data under their law;
- the possibility for the data subject to have an effective remedy before an independent authority.

CONCLUSIONS

40. The CJ-PD requested that the CDCJ submit the following recommendations to the Committee of Ministers:

a) this third evaluation should not recommend any revision of Recommendation No. R (87) 15 regulating the use of personal data in the police sector, in view of the fact that it was considered that the principles laid down by this Recommendation are still relevant today and continue to provide a basis for the elaboration of regulations on this issue and serve as the point of reference for any activities in this field. Furthermore, this Recommendation is referred to in other international instruments such as the Schengen Agreement and the Europol Convention.

b) the third evaluation of Recommendation No. (87) 15 should be the last of the periodic evaluations on the relevance of this recommendation, which until now have been carried out every four years;

c) the use of personal data in the police sector remains a continuing concern and therefore, where necessary, future evaluations of specific issues arising in relation to the development of new techniques of processing police data could be carried out;

d) taking the two recommendations above into account, the CJ-PD requests that the CDCJ request the Committee of Ministers to take a decision to the effect that this third evaluation should be the last of the periodic evaluations carried out by the CJ-PD on Recommendation No. R (87) 15 but that, where necessary, further evaluations on specific issues should be carried out;

41. The CJ-PD, in the course of its third evaluation of Recommendation No. (87) 15, reached the following conclusions. It submits them to the Committee of Ministers and requests authorisation to publish this report on the website of the Council of Europe:

[5] See for instance Article 18.3 of the Europol Convention.

I. Distinctions between judicial and police data:
In order to make a distinction between judicial and police data, it would be advisable to make explicit who is the controller of the file in the sense of Article 2, paragraph 2, littera d. of Convention 108, with regard to judicial data and police data. The controller of the file in this sense need not necessarily be the same as the authority who, according to the code of criminal procedure, is responsible for making decisions on or conducting criminal investigations. Special care should be taken to avoid loopholes in responsibility, in particular when personal data are collected and used by the police following an order from the judiciary to use intrusive surveillance methods such as interception of telecommunications.

II. Permanent files:
It would be advisable when setting up a permanent file to specify its purpose and the criteria for inclusion of personal data to the supervisory authority in order to enable the data subject to foresee whether his data may be included.

III. Ad hoc files for the analysis of specific criminal phenomena:
The collection of data for an ad hoc file set up for the analysis of specific criminal phenomena is bound by the purpose of the file. This could lead to a file containing an indeterminate type of data, not least in order to avoid the risk of excluding exculpatory evidence. The indiscriminate use of such data, whatever the police purpose they are used for, could have the same effect as overall surveillance of the data subject and therefore could lead to an arbitrary interference in their rights and fundamental freedoms, in particular their right to privacy. The use of personal data contained in such an ad hoc file for the purposes of another ad hoc file set up for a specific inquiry could only be considered compatible with the original purpose for which the first file was set up when there is a concrete link between the two files or between the personal data contained in the files that justifies such use. Data, for example the results of a telecommunications intercept or the seizure of a hard disk, that are apparently irrelevant for the purpose should be deleted or returned.

IV. Ad hoc files for analysis of specific criminal phenomena
It would be advisable that ad hoc files established for the purpose of analysis of a specific criminal phenomenon define the categories of persons about whom data may be stored and the categories of data about them with a certain degree of precision. In the case of serious criminal phenomena, it may be necessary to compare two such ad hoc files. Where, by comparison, concrete links are established, data from the first ad hoc file could be used also for the purposes of the second ad hoc file and vice versa.

V. Index systems:
Risks to rights and fundamental freedoms, in particular the right to privacy, which result from ad hoc files could be countered by compensatory substantive and procedural safeguards with regard to the use of the data. In particular, specific rules should regulate the use of an index system which enables access to data in the different ad hoc files. These rules should balance the obligation to protect the rights and fundamental freedoms, in particular the right to privacy with the necessity of using the data to combat crime effectively.

VI. Incompatible use:
The search for personal data in ad hoc files that cannot be regarded as a form of compatible use should be regulated in accordance with Article 9 of Convention 108 in the national code of criminal procedure or other laws.

VII. The categories of persons about which data may be stored:

It would be advisable to specify the categories of persons about whom data may be collected and stored, as well as the kind of information that may be recorded. These categories should be defined with enough precision in order that individuals can reasonably foresee whether they fall under the scope of these categories or not.

Personal data about third parties to the criminal investigation should only be collected and stored when necessary for the purpose for which a file was set up.

It would be advisable to specify the categories of third parties whose data may be collected and stored because they have a certain relationship with the persons who are the principal subjects of the criminal investigation or because the collection of their data is necessary in order to meet the requirements of a fair trial.

It would be advisable to provide for a periodic review of the data stored in order to establish the adequacy of the category under which they are stored.

VIII. Length of storage and deletion of data:

The length of storage of personal data processed by the police should be established on the basis of the principle of necessity in relation to the purposes for which those data were stored.

In the case law of some national data protection supervisory authorities, "necessary" is strictly interpreted as something which is indispensable (in order to be collected, for instance). However, information which may be considered necessary at the time of its collection by a judicial authority may subsequently be found to be irrelevant in the light of developments in the inquiry. It would be advisable to fix maximum storage periods for the different categories of personal data processed by the police as far as possible, for the transparency of the legal system. Periodic reviews of the quality of personal data should be carried out in every case. When data are no longer necessary to fulfil the requirements of the police purposes for which they were collected, they should be deleted or be kept for the purposes of historical, scientific or statistical research. Their storage should be accompanied by safeguards and security measures to prevent their use for other purposes. In exceptional cases and in accordance with Article 9 of Convention 108, domestic law could lay down conditions for the re-use of these data for police purposes if these data are necessary for review procedures or for a concrete criminal investigation.