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
Report
a) Distinctions between police and judicial data
b) Types of files held by the police
c) The categories of persons about whom data may be stored
d) Length of storage and deletion of data
e) Screening of individuals
f) Transfer of data to third countries which do not ensure an adequate level of protection
Conclusions

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).

---

[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).

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.

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

[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.

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:

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.