Recommendation No.R (87) 15

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR
(Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,
Considering that the aim of the Council of Europe is to achieve a greater unity between its members;
Aware of the increasing use of automatically processed personal data in the police sector and of the possible benefits obtained through the use of computers and other technical means in this field;
Taking account also of concern about the possible threat to the privacy of the individual arising through the misuse of automated processing methods;
Recognising the need to balance the interests of society in the prevention and suppression of criminal offences and the maintenance of public order on the one hand and the interests of the individual and his right to privacy on the other;
Bearing in mind the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and in particular the derogations permitted under Article 9;
Aware also of the provisions of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms,
Recommends the governments of member states to:
- be guided in their domestic law and practice by the principles appended to this Recommendation, and
- ensure publicity for the provisions appended to this Recommendation and in particular for the rights which its application confers on individuals.

Appendix to Recommendation No. R (87) 15

Scope and definitions

The principles contained in this Recommendation apply to the collection, storage, use and communication of personal data for police purposes which are the subject of automatic processing.
For the purposes of this Recommendation, the expression "personal data" covers any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time, cost and manpower.
The expression "for police purposes" covers all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order.
The expression "responsible body" (controller of the file) denotes the authority, service or any other public body which is competent according to national law to decide on the purpose of an automated file, the categories of personal data which must be stored and the operations which are to be applied to them.
A member state may extend the principles contained in this Recommendation to personal data not undergoing automatic processing.

Manual processing of data should not take place if the aim is to avoid the provisions of this Recommendation.
A member state may extend the principles contained in this Recommendation to data relating to groups of persons, associations, foundations, companies, corporations or any other body consisting directly or indirectly of individuals, whether or not such bodies possess legal personality.
The provisions of this Recommendation should not be interpreted as limiting or otherwise affecting the possibility for a member state to extend, where appropriate, certain of these principles to the collection, storage and use of personal data for purposes of state security.

Basic principles

Principle 1 - Control and notification

1.1. Each member state should have an independent supervisory authority outside the police sector which should be responsible for ensuring respect for the principles contained in this Recommendation.
1.2. New technical means for data processing may only be introduced if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation.
1.3. The responsible body should consult the supervisory authority in advance in any case where the introduction of automatic processing methods raises questions about the application of this Recommendation.
1.4. Permanent automated files should be notified to the supervisory authority. The notification should specify the nature of each file declared, the body responsible for its processing, its purposes, the type of data contained in the file and the persons to whom the data are communicated.
Ad hoc files which have been set up at the time of particular inquiries should also be notified to the supervisory authority either in accordance with the conditions settled with the latter, taking account of the specific nature of these files, or in accordance with national legislation.

Principle 2 - Collection of data

2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.
2.2. Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.
2.3. The collection of data by technical surveillance or other automated means should be provided for in specific provisions.
2.4. The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry.

Principle 3 - Storage of data

3.1. As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their

lawful tasks within the framework of national law and their obligations arising from international law.
3.2. As far as possible, the different categories of data stored should be distinguished in accordance with their degree of accuracy or reliability and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments.
3.3. Where data which have been collected for administrative purposes are to be stored permanently, they should be stored in a separate file. In any case, measures should be taken so that administrative data are not subject to rules applicable to police data.

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

Principle 5 - Communication of data
5.1. Communication within the police sector
The communication of data between police bodies to be used for police purposes should only be permissible if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.
5.2.i. Communication to other public bodies
Communication of data to other public bodies should only be permissible if, in a particular case:

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

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

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

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

> *a.* the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if

b. the communication is necessary so as to prevent a serious and imminent danger.

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

a. if there exists a clear legal provision under national or international law,

b. in the absence of such a provision, if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law,

and provided that domestic regulations for the protection of the person are not prejudiced.
5.5.i. Requests for communication
Subject to specific provisions contained in national legislation or in international agreements, requests for communication of data should provide indications as to the body or person requesting them as well as the reason for the request and its objective.
5.5.ii. Conditions for communication
As far as possible, the quality of data should be verified at the latest at the time of their communication. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated and data based on opinions or personal assessments checked at source before being communicated and their degree of accuracy or reliability indicated.
If it is discovered that the data are no longer accurate and up to date, they should not be communicated. If data which are no longer accurate or up to date have been communicated, the communicating body should inform as far as possible all the recipients of the data of their nonconformity.
5.5.iii. Safeguards for communication
The data communicated to other public bodies, private parties and foreign authorities should not be used for purposes other than those specified in the request for communication.
Use of the data for other purposes should, without prejudice to paragraphs 5.2 to 5.4 of this principle, be made subject to the agreement of the communicating body.
5.6. Interconnection of files and on-line access to files
The interconnection of files with files held for different purposes is subject to either of the following conditions:

a. the grant of an authorisation by the supervisory body for the purposes of an inquiry into a particular offence, or

b. in compliance with a clear legal provision.

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

Principle 6 - Publicity, right of access to police files, right of rectification and right of appeal
6.1. The supervisory authority should take measures so as to satisfy itself that the public is informed of the existence of files which are the subject of notification as well as of its rights

in regard to these files. Implementation of this principle should take account of the specific nature of ad hoc files, in particular the need to avoid serious prejudice to the performance of a legal task of the police bodies.
6.2. The data subject should be able to obtain access to a police file at reasonable intervals and without excessive delay in accordance with the arrangements provided for by domestic law.
6.3. The data subject should be able to obtain, where appropriate, rectification of his data which are contained in a file.
Personal data which the exercise of the right of access reveals to be inaccurate or which are found to be excessive, inaccurate or irrelevant in application of any of the other principles contained in this Recommendation should be erased or corrected or else be the subject of a corrective statement added to the file.
Such erasure or corrective measures should extend as far as possible to all documents accompanying the police file and, if not done immediately, should be carried out, at the latest, at the time of subsequent processing of the data or of their next communication.
6.4. Exercise of the rights of access, rectification and erasure should only be restricted insofar as a restriction is indispensable for the performance of a legal task of the police or is necessary for the protection of the data subject or the rights and freedoms of others.
In the interests of the data subject, a written statement can be excluded by law for specific cases.
6.5. A refusal or a restriction of those rights should be reasoned in writing. It should only be possible to refuse to communicate the reasons insofar as this is indispensable for the performance of a legal task of the police or is necessary for the protection of the rights and freedoms of others.
6.6. Where access is refused, the data subject should be able to appeal to the supervisory authority or to another independent body which shall satisfy itself that the refusal is well founded.

Principle 7 - Length of storage and updating of data
7.1. Measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored.
For this purpose, consideration shall in particular be given to the following criteria: the need to retain data in the light of the conclusion of an inquiry into a particular case; a final judicial decision, in particular an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject; particular categories of data.
7.2. Rules aimed at fixing storage periods for the different categories of personal data as well as regular checks on their quality should be established in agreement with the supervisory authority or in accordance with domestic law.

Principle 8 - Data security
8. The responsible body should take all the necessary measures to ensure the appropriate physical and logical security of the data and prevent unauthorised access, communication or alteration.
The different characteristics and contents of files should, for this purpose, be taken into account.