COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

RECOMMENDATION No. R (91) 10

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES

ON THE COMMUNICATION TO THIRD PARTIES OF PERSONAL DATA HELD BY PUBLIC BODIES[1]

(Adopted by the Committee of Ministers on 9 September 1991 at the 461st 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 greater unity between its members;

Noting that automatic data processing has enabled public bodies to store on electronic files the data, including personal data, which they collect for the purposes of discharging their functions;

Aware of the fact that the new automated techniques for the storage of such data greatly facilitate third party access to them, thus contributing to the greater circulation of information within society, which the Committee of Ministers has encouraged in its Recommendation No. R (81) 19 on the access to information held by public authorities as well as in its Declaration of 29 April 1982 on freedom of expression and information;

Believing however that automation of data collected and stored by public bodies makes it necessary to address its impact on personal data or personal data files which are collected and stored by public bodies for the discharge of their functions;

Noting in particular that the automation of personal data files has increased the risk of infringement of privacy since it allows greater access by telematic means to personal data files held by public bodies as well as communication of such data or personal data files to third parties;

Mindful in this regard of the increasing tendencies on the part of the private sector to exploit for commercial advantage the personal data or personal data files held by public bodies as well as the emergence of policies within public bodies envisaging communication by electronic means of personal data or personal data files to third parties on a commercial basis;

Determined therefore to promote data protection principles based on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[2] so as to ensure that the

---

1. When this recommendation was adopted, and in application of Article 10.2.*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 or not with Principles 6.2, 6.3, paragraph 2, and 7.1 of the appendix to the recommendation;

— the Representatives of Norway and the United Kingdom reserved the right of their Governments to comply or not with Principles 6.2 and 6.3, paragraph 2, of the appendix to the recommendation;

— the Representative of Sweden reserved the right of his Government to comply or not with paragraph 6.2 of the appendix to the recommendation.

2. Strasbourg, 1981, European Treaty Series No. 108 (hereinafter called Convention No. 108).

communication by public bodies of personal data or personal data files to third parties, in particular by electronic means, has its basis in law and is accompanied by safeguards for the data subject;

Noting in particular that these data protection principles should be reflected in the new automated context which now characterises the communication of personal data or personal data files to third parties under legal provisions governing accessibility by third parties to personal data or personal data files,

Recommends that the governments of the member states:

i. take account of the principles contained in the appendix to this recommendation whenever personal data or personal data files collected and stored by public bodies may be made accessible to third parties;

ii. have due regard to the principles contained in the appendix to this recommendation in their law and practice regarding the automation and communication to third parties by electronic means of personal data or personal data files;

iii. ensure wide circulation of the principles contained in the appendix to this recommendation among public bodies;

iv. bring the principles contained in the appendix to this recommendation to the attention of authorities set up under data protection legislation or legislation on access to public-sector information.

Appendix to Recommendation No. R (91) 10

1. *Scope and definitions*

1.1. The principles contained in this recommendation apply to the automatic processing of personal data which are collected by public bodies and which may be communicated to third parties.

1.2. Member states may extend the scope of this recommendation so as to include data relating to groups, companies, associations, etc., regardless of whether or not they possess legal personality, as well as to personal data in non-automated form.

For the purposes of this recommendation:

1.3. — the expression "personal data" refers to any information relating to an identified or identifiable individual (data subject). An individual shall not be regarded as "identifiable" if the identification requires an unreasonable amount of time, cost and manpower;

— the expression "public bodies" refers to any administration, institution, establishment or other body which exercises public service or public interest functions as a consequence of it being invested with public powers.

Domestic law may broaden the scope of the expression "public bodies".

— the expression "files accessible to third parties" refers to files held by public bodies containing personal data which may be communicated to the public or to third parties having a particular interest and which are in accordance with general laws on access to public-sector information or freedom of information, constitutional provisions as well as specific laws, regulations or case-law which authorise third parties to have access to information held by public bodies, including by means of official publication;

— the expression "communication" refers to making files or personal data accessible, such as by authorising their consultation, transmitting them, disseminating them or making them available regardless of the means or media used;

— the expression "third parties" refers to legal and natural persons to whom personal data are communicated by public bodies to the exclusion of other public bodies.

Domestic law may broaden the scope of the expression "third parties".

2. *Respect for privacy and data protection principles*

2.1. The communication, in particular by electronic means, of personal data or personal data files by public bodies to third parties should be accompanied by safeguards and guarantees designed to ensure that the privacy of the data subject is not unduly prejudiced.

In particular, the communication of personal data or personal data files to third parties should not take place unless:

a. a specific law so provides; or

b. the public has access thereto under legal provisions governing access to public-sector information; or

c. the communication is in conformity with domestic legislation on data protection; or

d. the data subject has given his free and informed consent.

2.2. Unless domestic law provides appropriate safeguards and guarantees for the data subject, personal data or personal data files may not be communicated to third parties for purposes incompatible with those for which the data were collected.

2.3. Domestic legislation on data protection should apply to the processing by a third party of personal data communicated to him by public bodies.

3. *Sensitive data*

3.1. Personal data falling within any of the categories referred to in Article 6 of Convention No. 108 should not be stored in a file or in part of a file generally accessible to third parties.

Any exception to this principle should be strictly provided for by law and accompanied by the appropriate safeguards and guarantees for the data subject.

3.2. The provisions of Principle 3.1 are without prejudice to the possibility of storing in files accessible to third parties categories of data which in other circumstances would be regarded as sensitive but which concern those data subjects in public life who perform functions which belong to the public domain and as a result their data are accessible to third parties.

4. *Generally accessible data*

4.1. The purposes for which the data will be collected and processed in files accessible to third parties as well as the public interest justifying their being made accessible should be indicated in accordance with domestic law and practice.

4.2. Before or at the time of the collection, the data subject should be informed in accordance with domestic law and practice of the compulsory or optional nature of the collection, of the legal bases and the purposes of the collection and processing of personal data as well as the public interest justifying their being made accessible.

4.3. Public bodies should be able to avoid the communication to third parties of personal data which are stored in a file accessible to the public and which concern data subjects whose security and privacy are particularly threatened.

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

5.1. The automated processing of personal data contained in files accessible to third parties should be carried out in accordance with domestic law.

Domestic law should lay down the conditions governing communication of and access to the data and, in particular, provide the conditions governing the automatic communication and on-line consultation of such data.

5.2. At the time of automatic communication, technical means designed to limit the scope of electronic interrogations or searches should be introduced with a view to preventing unauthorised downloading or consultation of personal data or files containing such data.

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

6.1. Where the data subject is legally obliged to provide his data for storage in files accessible to third parties, the processing of personal data by third parties should either be subject to obtaining the express and informed consent of the data subject or be in accordance with statutory requirements.

Where the consent requirement applies, the data subject should be able to withdraw his consent at any time.

6.2. Where the storage of the personal data in a file accessible to third parties is not obligatory, the data subject should be informed before or at the time of the collection of his right:

a. not to have his data stored in a file accessible to third parties; or

b. to have his data stored in such a file and communicated without however their being processed by third parties; or

c. to object to his data continuing to be processed by third parties; or

d. to have his data deleted at any time.

6.3. If a third party creates files containing personal data obtained from files accessible to third parties, such files should be subject to the requirements of domestic legislation on data protection, including the rights of the data subject.

In particular, the data subject should be able to know of the existence of the new file, of its purpose and of his right to have his data erased from the file in question.

7. *File interconnection/matching*

Unless permitted by domestic law providing appropriate safeguards, the interconnection — in particular by means of connecting, merging or downloading — of personal data files consisting of personal data originating from files accessible to third parties with a view to producing new files, as well as the matching or interconnection of files or personal data held by third parties with one or more files held by public bodies so as to enrich the existing files or data, should be prohibited.

8. *Transborder data flows*

8.1. The principles of this recommendation are applicable to the transborder communication of personal data which are collected by public bodies and which may be communicated to third parties.

8.2. The transborder communication of personal data to third parties residing in a state which has ratified Convention No. 108 and which thus has a data-protection law should not be subjected to special conditions concerning the protection of privacy.

8.3. Where the principle of equivalent protection is respected, no restriction should be placed on the transborder communication of personal data to third parties residing in a state which has not ratified Convention No. 108 but which has legal provisions which are in conformity with the principles of that convention and of this recommendation.

8.4. Unless otherwise provided for by domestic law, the transborder communication of personal data to third parties residing in a state the legal provisions of which are not in conformity with Convention No. 108 or with this recommendation should not as a rule occur unless:

a. necessary measures, including of a contractual nature, to respect the principles of the convention and this recommendation have been taken and the data subject has the possibility to object to communication, or

b. the data subject has given his free and informed consent in writing and has the possibility to withdraw his consent at any time.

8.5. Measures should be taken to avoid personal data or files containing such data being subjected to automatic transborder communication to third parties without the knowledge of the data subjects.

9. *Co-ordination/co-operation*

Where general legislation governing access to public-sector information provides for the establishment of a supervisory body to implement such legislation and there exists at the same time general data-protection legislation with a separate authority responsible for the implementation of that legislation, the respective authorities should come to an arrangement designed to facilitate the exchange of information relating to the conditions governing communication of personal data originating in files accessible to third parties.