COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

Recommendation Rec(2002)9
of the Committee of Ministers to member states
on the protection of personal data collected and processed for insurance purposes

(Adopted by the Committee of Ministers on 18 September 2002
at the 808th meeting of the Ministers' Deputies)

Preamble

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

1. Considering that the aim of the Council of Europe is to achieve greater unity among its members;

2. Recalling the general principles relating to data protection of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), and in particular Article 6, which states that personal data categorised as sensitive may not be processed unless domestic law provides appropriate safeguards;

3. Aware of the fact that automated processing of personal data for insurance purposes is increasingly widespread, not only for the preparation, conclusion, implementation and termination of insurance, but also to facilitate rational and economic management of insurance and to fight against fraud;

4. Aware of the fact that insurance is provided by various economic entities, in particular by insurance companies;

5. Convinced of the importance that the quality, integrity and availability of personal data have for insured persons;

6. Noting that virtually the entire population of the member states is affected by one or more insurance contract and that, for this reason, insurance professionals are in possession of a large volume of personal data, some of which are sensitive;

7. Convinced that it is desirable to regulate the collection and processing of personal data for insurance purposes, to guarantee their confidential character and data security and to ensure that the use to which they are put respects fundamental human rights and freedoms, notably the right to privacy;

8. Taking into account the fact that the mobility of individuals and the globalisation of markets and commercial activities necessitate a transborder exchange of information in the insurance sector also and require equivalent data protection in all the member states of the Council of Europe,

Recommends that governments of member states:

1. take measures to ensure that the principles contained in the appendix to this recommendation are reflected in their law and practice;

2. ensure wide circulation of the principles contained in the appendix to this recommendation among persons, public authorities and public or private bodies that collect and process personal data for insurance purposes, as well as to bodies with competence in data protection;

3. promote the acceptance and implementation of the principles contained in the appendix to this recommendation, notably by adopting legal provisions or encouraging the drafting of a code of ethics.

Appendix to Recommendation Rec(2002)9

1. Definitions

For the purposes of this recommendation:

a. "Personal data" covers any information relating to an identified or identifiable individual ("data subject"). An individual should not be regarded as "identifiable" if identification requires an unreasonable amount of time and manpower.

b. "Sensitive data" means personal data revealing racial origin, political opinions, religious or other beliefs, as well as personal data concerning health and sexual life. Data concerning criminal proceedings and convictions and other data defined as sensitive by domestic law are also considered to be sensitive data.

c. "For insurance purposes" comprises any operation involving the collection and processing of personal data relating to cover for a risk, in particular under a policy or an insurance contract.

d. "Processing" means any operation or set of operations carried out partly or completely with the help of automated processes and applied to personal data, such as recording, conservation or alteration, extraction, consultation, utilisation, communication, matching or interconnection and erasure or destruction.

e. "Communication" refers to the act of making personal data accessible to third parties, regardless of the means or media used.

f. "Controller" means the natural or legal person, public authority, agency, or any other body which, alone, or in collaboration with others, determines the purposes of and means used in the collection and processing of personal data.

g. "Processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

2. Scope

2.1. This Recommendation applies to personal data collected and processed for insurance purposes. It does not apply to the collection and processing of personal data used for social security purposes.

2.2. Member states are encouraged to extend the application of this recommendation to non-automated processing of personal data for insurance purposes.

2.3. No personal data should be processed in a non-automated manner in order to avoid applying the principles of this Recommendation.

2.4. Member states may extend the application of the principles set out in this Recommendation to the collection and processing of data relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality.

2.5. Member states may extend the principles set out in this recommendation to the protection of personal data used for social security purposes.

3. Respect for privacy

3.1. Respect for fundamental rights and freedoms, particularly the right to private life, must be safeguarded when personal data are collected and processed for insurance purposes.

3.2. Persons who, in the course of an insurance activity, have access to personal data must, in accordance with domestic law and practice, be subject to rules of confidentiality. Moreover, the collection and processing of medical data must only be undertaken by health professionals or in conformity either with confidentiality rules comparable to those applicable to health-care professionals or with equally effective safeguards provided for in domestic law.

4. Collection and processing of personal data for insurance purposes

Essential conditions for the collection and processing of personal data

4.1. The collection and processing (including communication) of personal data should be carried out fairly and lawfully and for specified and lawful purposes,

Personal data should be

– adequate, relevant and not excessive in relation to the purposes for which they are collected or for which they are to be further processed;

– accurate and, if necessary, kept up to date.

Source of personal data

4.2. Personal data collected and processed for insurance purposes should, in principle, be collected from the data subject or his/her legal representative.

Lawfulness

4.3. Personal data may be collected and processed for insurance purposes:

a. if provided for by law;

b. for the performance of an insurance contract to which the data subject is party, as well as for the preparation of such a contract at the request of the data subject;

c. if the data subject or his/her legal representative or an authority or any other person or body provided for by law has given his/her consent as provided for in Chapter 6; or

d. if the data are necessary in the pursuit of the controller's legitimate interests, provided that these are not overridden by the interests of the data subject.

Purpose

4.4. Subject to the provisions of Principles 4.6 to 4.8, 8.1 and 13.1, personal data may only be collected and processed for the purposes of:

a. preparing and issuing insurance;
b. collecting premiums and submitting other bills;
c. settling claims or paying other benefits;
d. reinsurance;
e. co-insurance;
f. preventing, detecting and/or prosecuting insurance fraud;
g. establishing, exercising or defending a legal claim;
h. meeting another specific legal or contractual obligation;
i. prospecting new insurance markets;
j. internal management;
k. actuarial activities.

These data may not be processed further for purposes incompatible with the original purpose of the collection.

Unborn children

4.5. Personal data concerning unborn children should enjoy a protection comparable to the protection of the personal data of a minor.

Unless otherwise provided for by domestic law, the holder of the parental responsibilities may act as the person legally entitled to act for the unborn child, the latter being a data subject.

Sensitive data

4.6. The collection and processing of sensitive data should be prohibited, unless, for one of the purposes set out in Principles 4.4, 4.8, 8.1 and 13.1:

a. the data subject or his/her legal representative or an authority or any other person or body appointed by law has explicitly given his/her consent as provided for in Chapter 6; or

b. it is permitted by law and

i. subject to appropriate safeguards, processing is necessary for the purpose of complying with the controller's other legal or contractual obligations; or

ii. processing is necessary for establishing, exercising or defending a legal claim; or

iii. the processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving his/her consent.

c. collection and processing are permitted, subject to appropriate safeguards, on grounds of an important public interest, and provided for by law or by virtue of a decision of an authority within the meaning of Principle 15.1.

Criminal data

4.7. By way of derogation from Principle 4.6, the collection and processing of data concerning criminal proceedings and convictions may be carried out for insurance purposes only if suitable specific safeguards are provided for by domestic law, and if the data are necessary to combat insurance fraud, for the granting of insurance or the payment of claims or any other insurance benefit.

Direct marketing

4.8. Provided that the data subject has been informed and has not objected, the controller may use, for the purposes of marketing and promoting its range of services, the data collected and recorded for insurance purposes. If, however, processing concerns sensitive data, the explicit consent of the data subject is required provided that this is not contrary to domestic law.

The data subject should be informed of the fact that if he/she refuses to consent to or objects to his/her data being used for marketing purposes this will not prejudice the decision to provide him/her with insurance cover or to allow him/her to continue benefiting from insurance cover already issued.

5. Information for the data subject

5.1. Data subjects should be informed of the following:

a. the purpose or purposes for which data are or will be processed;

b. the identity of the controller;

c. any other information which is necessary to ensure the fairness of processing, such as:

– the categories of data collected or to be collected;

– the categories of external persons or bodies to whom, and the purposes for which, the data may be communicated;

– the possibility, if any, for data subjects to refuse their consent or to withdraw it and the consequences of such withdrawal;

– the conditions under which the rights of access and of rectification may be exercised;

– the individuals or bodies from whom the data are or will be collected;

– the obligatory or optional character of the reply to the questions which are the object of the collection and the consequences of a defective response with regard to the person.

5.2. Where the data are collected from the data subject, the controller should give data subjects the information listed in Principle 5.1 above at the latest at the time of collection, except where the data subject has already been informed.

5.3. Where personal data are not collected from data subjects, the controller should give the data subjects the information listed in Principle 5.1, as soon as the data are recorded or, if it is planned to communicate the data to a third party, at the latest when the data are first communicated.

The obligation to inform the data subject does not apply if:

a. the data subject has already been informed;

b. it proves impossible to provide the information or if it would involve disproportionate effort;

c. the processing or communication of the data for insurance purposes is expressly provided for by domestic law.

In the cases set out in *b* and *c*, appropriate safeguards must be provided for.

5.4. Information for the data subject must be appropriate and adapted to the circumstances.

5.5. If data subjects have no legal capacity and are unable to make their own decisions freely, and if domestic law does not permit them to act on their own behalf, the information must be provided to the persons legally empowered to act on behalf of those data subjects.

5.6. The provision of information to data subjects may be restricted if this is provided for by law and is necessary to prevent, investigate or prosecute a criminal offence or to guarantee the rights and liberties of others.

6. Consent

6.1. When data subjects are asked to give their consent, it must be freely given, specific and informed. Moreover, it must be unambiguous or, in the case of sensitive data, explicit.

However, there may be circumstances in which domestic law does not permit consent to be considered as a sufficient basis for lawfulness of collection or processing.

6.2. When personal data concern persons with no legal capacity and when domestic law does not permit the data subject to act on his/her own behalf, consent is required of his/her legal representative or an authority or any other person or body appointed by law.

6.3. If, in accordance with Principle 5.5 above, data subjects with no legal capacity have been informed of the intention to collect and process data concerning them, their wishes should be taken into consideration, provided that this is not contrary to domestic law.

7. Collection and processing by processors

7.1. In accordance with the provisions of domestic law, controllers may contract out the collection and processing of personal data for a specific purpose, in so far as they are authorised to collect and process these data and the processor undertakes to act solely on instruction from the controller and to respect the provisions of domestic law which implement Chapter 11 of the Appendix to this Recommendation.

7.2. Controllers should choose processors who offer adequate safeguards regarding the technical and organisational aspects of the processing to be carried out. They must ensure that these safeguards are observed and that, in particular, the processing is in accordance with their instructions.

7.3. The collection and processing of personal data by processors should be governed by a contract or legal instrument binding the processor to the controller and specifying that the processor will only act within the terms of reference issued by the controller and the provisions of domestic law concerning the obligations of processors.

8. Communication of data for other purposes

8.1. Personal data may only be communicated for purposes other than those laid down in Principle 4.4 if:

a. this is provided for in domestic law and constitutes a necessary measure in a democratic society for preventing, investigating and prosecuting a criminal offence or for guaranteeing another important public interest, or

b. data subjects or their legal representatives or an authority or any other person or body appointed by law have given their consent as provided for in Chapter 6, or

c. communication is for purposes of direct marketing, provided that the data subject has been informed and has no objection. However, the data subject's explicit consent should be required if the data to be communicated are of a sensitive nature as provided for in Chapter 6; or

d. the data are necessary in the pursuit of the controller's legitimate interests, provided that these are not overridden by the interests of the data subject. However the data subject's explicit consent should be required if the data to be communicated are of a sensitive nature as provided for in Chapter 6.

9. Individual automated decisions

9.1. Insurance decisions which have a legal effect on data subjects or affect them significantly should not be taken solely on the basis of automated data processing intended to evaluate certain personal aspects relating to them according to pre-established criteria or statistical results.

9.2. Such decisions may nevertheless be taken if they satisfy a request made by the data subjects with a view to the conclusion or execution of an insurance contract, or if the data subjects are permitted to put their point of view in order to guarantee protection of their legitimate interests. Such decisions may also be taken if they are authorised by a law which safeguards the legitimate interests of the data subject.

10. Rights of access and rectification

10.1. All data subjects should, on request, be able to obtain confirmation as to whether data relating to them are being processed or not and, in an intelligible form, to obtain all of the data concerning them, as well as information at least as to the purposes of the processing operation, the categories of data concerned by the processing, the recipients or categories of recipients to whom the data are communicated, and the source of the data. They should also be informed, on request, of the logic underlying the automated processing of data concerning them, at least in the case of individual automated decisions.

10.2. The rights of data subjects to obtain data concerning them should not be restricted unless this is provided for by law and is necessary:

a. for preventing, investigating or prosecuting a criminal offence;

b. to guarantee the rights and liberties of data subjects or others.

In that case, the right of access may be restricted only for as long as the reason for the restriction remains.

10.3. Data subjects should be entitled to have their data rectified, blocked or erased as appropriate where they have been collected or processed in disregard of the provisions of domestic law implementing the principles of this Recommendation and, in particular, where they are found to be inaccurate, irrelevant or excessive.

10.4. Reasons for restriction of the rights of access, rectification, erasure and blocking should be given in writing. Where the data subject's rights of access, rectification, erasure and blocking of data are restricted, the data subject should be informed of his/her right to ask the competent authority to check the lawfulness of data processing.

10.5. Third parties to whom data have been communicated should be informed of the rectification, erasure or blocking carried out unless this is manifestly unreasonable or unfeasible.

10.6. Controllers should communicate at reasonable intervals and without excessive delay or expense to persons who exercise the right of access to personal data concerning them, as well as any information referred to in Principle 10.1 for which access is requested.

11. Security of data

11.1. Appropriate technical and organisational measures should be taken to protect personal data – processed in accordance with the provisions of domestic law giving effect to the principles of this Recommendation – against accidental or unlawful destruction, accidental loss, as well as against unauthorised access, alteration or communication or any other form of unlawful processing.

Such measures should ensure an appropriate level of security taking account, on the one hand, of the technical state of the art and, on the other hand, of the sensitive nature of data collected and processed for insurance purposes and the evaluation of potential risks. These measures should be reviewed periodically.

11.2. In order to ensure, in particular, the confidentiality, integrity and availability of processed data, as well as the protection of data subjects, the controller should take appropriate measures:

a. to prevent any unauthorised person from having access to installations used for processing personal data (control at the entrance to installations);

b. to prevent data media from being read, copied, altered or removed by unauthorised persons (control of data media);

c. to prevent the unauthorised entry of data into the information system, and any unauthorised consultation, modification or deletion of memorised personal data (memory control);

d. to prevent automated data processing systems from being used by unauthorised persons by means of data transmission equipment (control of utilisation);

e. with a view to, on the one hand, selective access to data and, on the other hand, the security of the personal data, to ensure that the processing as a general rule is so designed as to enable the separation of:

- identifiers and data relating to the identity of persons,
- administrative data,
- sensitive data (access control);

f. to guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment (control of communication);

g. to guarantee that it is possible to check and establish, *a posteriori*, who has had access to the system and what personal data have been introduced into the information system, when and by whom (control of data introduction);

h. to prevent the unauthorised reading, copying, alteration or deletion of personal data during the communication of personal data and the transport of data media (control of transport);

i. to safeguard data by making security copies (availability control).

11.3. Controllers should, in accordance with domestic law, draw up appropriate internal regulations which respect the related principles in this Recommendation.

11.4. Where necessary, controllers should appoint an independent person responsible for information systems security and data protection and competent for giving advice on these issues.

12. Transborder data flows

12.1. The principles of this Recommendation are applicable to the transborder flow of personal data collected and processed for insurance purposes.

12.2. The transborder flow of personal data to a state which has ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), and which has legislation which provides at least equivalent data protection, should not be subjected to special conditions concerning the protection of privacy.

12.3. No restriction should be placed on the transborder flow of data to a state which has not ratified the Convention but which ensures an adequate level of protection.

12.4. Unless otherwise provided for by domestic law, the transborder flow of data to a state which does not ensure an adequate level of protection should not as a rule occur unless:

a. the data subject has given his/her consent as provided for in Chapter 6, or

b. measures, including those of a contractual nature, necessary to respect the provisions of domestic law giving effect to the principles of the Convention and this Recommendation, have been taken, and the data subject has the possibility to object to the transfer.

13. Conservation of data

13.1. Where personal data are no longer necessary for the accomplishment of the purposes for which they were collected and processed by the controller, they should be deleted. This principle also applies where a decision is taken to refuse insurance coverage. If they must nevertheless be conserved for purposes of scientific research or statistics, or other purposes provided for by law, they should be conserved separately and be accessible only for these purposes subject to appropriate safeguards.

13.2. In determining the period of conservation of data, account should be taken in particular of the need to retain data for the period necessary for the purpose of defending legal actions or for furnishing proof of transactions or for justifying a decision to refuse insurance coverage.

14. Remedies

Domestic law should provide appropriate sanctions and remedies in cases of breach of the provisions of domestic law giving effect to the principles laid down in this Recommendation.

15. Ensuring respect for the principles

15.1. Member states should give one or more authorities responsibility for ensuring in complete independence the application of the provisions of domestic law giving effect to the principles laid down in this Recommendation.

15.2. The following information should be publicised appropriately and be readily available to all:

a. the name and address of the controller and of his representative, if any;

b. the purpose or purposes of the processing;

c. the category or categories of data subject and of the data;

d. the recipient or categories of recipient to whom the data might be disclosed;

e. any proposed transfers of data to third countries.