

**Recommendation CM/Rec(2010)13
of the Committee of Ministers to member states
on the protection of individuals with regard to automatic processing
of personal data in the context of profiling¹**

*(Adopted by the Committee of Ministers on 23 November 2010
at the 1099th meeting of the Ministers' Deputies)*

The Committee of Ministers,

Considering that the aim of the Council of Europe is to achieve ever closer union among its members;

Noting that information and communication technologies (ICTs) allow the collection and processing on a large scale of data, including personal data, in both the private and public sectors; noting that ICTs are used for a wide range of purposes including uses for services widely accepted and valued by society, consumers and the economy; noting at the same time that continuous development of convergent technologies poses new challenges as regards collection and further processing of data;

Noting that this collection and processing may occur in different situations for different purposes and concern different types of data, such as traffic data and user queries on the Internet, consumer buying habits, activities, lifestyle and behaviour data concerning users of telecommunication devices including geo-location data, as well as data stemming in particular from social networks, video surveillance systems, biometric systems and radio frequency identification (RFID) systems foreshadowing the "Internet of things"; noting that it is desirable to assess the different situations and purposes in a differentiated manner;

Noting that data thus collected are processed namely by calculation, comparison and statistical correlation software, with the aim of producing profiles that could be used in many ways for different purposes and uses by matching the data of several individuals; noting that the development of ICTs enables these operations to be performed at a relatively low cost;

Considering that, through this linking of a large number of individual, even anonymous, observations, the profiling technique is capable of having an impact on the people concerned by placing them in predetermined categories, very often without their knowledge;

Considering that profiles, when they are attributed to a data subject, make it possible to generate new personal data which are not those which the data subject has communicated to the controller or which she or he can reasonably presume to be known to the controller;

Considering that the lack of transparency, or even "invisibility", of profiling and the lack of accuracy that may derive from the automatic application of pre-established rules of inference can pose significant risks for the individual's rights and freedoms;

Considering in particular that the protection of fundamental rights, in particular the right to privacy and protection of personal data, entails the existence of different and independent spheres of life where each individual can control the use she or he makes of her or his identity;

Considering that profiling may be in the legitimate interests of both the person who uses it and the person to whom it is applied, such as by leading to better market segmentation, permitting an analysis of risks and fraud, or adapting offers to meet demand by the provision of better services; and considering that profiling may thus provide benefits for users, the economy and society at large;

Considering, however, that profiling an individual may result in unjustifiably depriving her or him from accessing certain goods or services and thereby violate the principle of non-discrimination;

¹ 1. When this recommendation was adopted:
- in accordance with Article 10.2.c of the Rules of Procedure of the Ministers' Deputies, the Representative of the United Kingdom reserved the right of her Government to comply with it or not.

Considering furthermore that profiling techniques, highlighting correlations between sensitive data in the sense of Article 6 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, hereafter "Convention No. 108") and other data, can enable the generation of new sensitive data concerning an identified or identifiable person; further considering that such profiling can expose individuals to particularly high risks of discrimination and attacks on their personal rights and dignity;

Considering that the profiling of children may have serious consequences for them throughout their life, and given that they are unable, on their own behalf, to give their free, specific and informed consent when personal data are collected for profiling purposes, specific and appropriate measures for the protection of children are necessary to take account of the best interests of the child and the development of their personality in accordance with the United Nations Convention on the Rights of the Child;

Considering that the use of profiles, even legitimately, without precautions and specific safeguards, could severely damage human dignity, as well as other fundamental rights and freedoms, including economic and social rights;

Convinced that it is therefore necessary to regulate profiling as regards the protection of personal data in order to safeguard the fundamental rights and freedoms of individuals, in particular the right to privacy, and to prevent discrimination on the basis of sex, racial and ethnic origin, religion or belief, disability, age or sexual orientation;

Recalling in this regard the general principles on data protection in Convention No. 108;

Recalling that every person shall have the right of access to data relating to him or her and considering that every person should know the logic involved in profiling; whereas this right should not affect the rights and freedoms of others, and in particular not adversely affect trade secrets or intellectual property or the copyright protecting the software;

Recalling the necessity to comply with the already existing principles set out by other relevant recommendations of the Council of Europe, in particular Recommendation Rec(2002)9 on the protection of personal data collected and processed for insurance purposes and Recommendation Rec(97)18 concerning the protection of personal data collected and processed for statistical purposes;

Taking into account the Council of Europe Convention on Cybercrime (ETS No. 185 – Budapest Convention) which contains regulations for the preservation, collection and exchange of data, subject to conditions and safeguards providing for the adequate protection of human rights and liberties;

Taking into account both Article 8 of the European Convention on Human Rights (ETS No. 5), as interpreted by the European Court of Human Rights, and new risks created by the use of information and communication technologies;

Considering that the protection of human dignity and other fundamental rights and freedoms in the context of profiling can be effective if, and only if, all the stakeholders contribute together to a fair and lawful profiling of individuals;

Taking into account that the mobility of individuals, the globalisation of markets and the use of new technologies necessitate transborder exchanges of information, including in the context of profiling, and require comparable data protection in all the member states of the Council of Europe,

Recommends that the governments of member states:

1. apply the appendix to the present recommendation to the collection and processing of personal data used in the context of profiling notably by taking measures to ensure that the principles set out in the appendix to this recommendation are reflected in their law and practice;

2. ensure the broad dissemination of the principles set out in the appendix to this recommendation among persons, public authorities and public or private bodies, particularly those which participate in and use profiling, such as designers and suppliers of software, profile designers, electronic communications service providers and information society service providers, as well as among the bodies responsible for data protection and the standardisation bodies;
3. encourage such persons, public authorities and public or private bodies to introduce and promote self-regulation mechanisms, such as codes of conduct, ensuring respect for privacy and data protection, and put in place the technologies found in the appendix to this recommendation.

Appendix to Recommendation CM/Rec(2010)13

1. Definitions

For the purposes of this recommendation:

- a. "Personal data" means any information relating to an identified or identifiable individual ("data subject"). An individual is not considered "identifiable" if identification requires unreasonable time or effort.
- b. "Sensitive data" means personal data revealing the racial origin, political opinions or religious or other beliefs, as well as personal data on health, sex life or criminal convictions, as well as other data defined as sensitive by domestic law.
- c. "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 storage, conservation, adaptation or alteration, extraction, consultation, utilisation, communication, matching or interconnection, as well as erasure or destruction.
- d. "Profile" refers to a set of data characterising a category of individuals that is intended to be applied to an individual.
- e. "Profiling" means an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.
- f. "Information society service" refers to any service, normally provided for remuneration, at a distance, by electronic means.
- g. "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.
- h. "Processor" means the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

2. General principles

- 2.1. The respect for fundamental rights and freedoms, notably the right to privacy and the principle of non-discrimination, shall be guaranteed during the collection and processing of personal data subject to this recommendation.
- 2.2. Member states should encourage the design and implementation of procedures and systems in accordance with privacy and data protection, already at their planning stage, notably through the use of privacy-enhancing technologies. They should also take appropriate measures against the development and use of technologies which are aimed, wholly or partly, at the illicit circumvention of technological measures protecting privacy.

3. Conditions for the collection and processing of personal data in the context of profiling

A. Lawfulness

3.1. The collection and processing of personal data in the context of profiling should be fair, lawful and proportionate, and for specified and legitimate purposes.

3.2. Personal data used in the context of profiling should be adequate, relevant and not excessive in relation to the purposes for which they are collected or for which they will be processed.

3.3. Personal data used in the context of profiling should be stored in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are collected and processed.

3.4. Collection and processing of personal data in the context of profiling may only be performed:

- a. if it is provided for by law; or
- b. if it is permitted by law and:

- the data subject or her or his legal representative has given her or his free, specific and informed consent;

- is necessary for the performance of a contract to which the data subject is a party or for the implementation of pre-contractual measures taken at the request of the data subject;

- is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the personal data are disclosed;

- is necessary for the purposes of the legitimate interests of the controller or the third party or parties to whom the profiles or data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subjects;

- is necessary in the vital interests of the data subject.

3.5. The collection and processing of personal data in the context of profiling of persons who cannot express on their own behalf their free, specific and informed consent should be forbidden except when this is in the legitimate interest of the data subject or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law.

3.6. When consent is required it is incumbent on the controller to prove that the data subject has agreed to profiling on an informed basis, as set out in Section 4.

3.7. As much as possible, and unless the service required necessitates knowledge of the data subject's identity, everyone should have access to information about goods or services or access to these goods or services themselves without having to communicate personal data to the goods or services provider. In order to ensure free, specific and informed consent to profiling, providers of information society services should ensure, by default, non-profiled access to information about their services.

3.8. The distribution and use, without the data subject's knowledge, of software aimed at the observation or the monitoring in the context of profiling of the use being made of a given terminal or electronic communication network should be permitted only if they are expressly provided for by domestic law and accompanied by appropriate safeguards.

B. Data quality

3.9. Appropriate measures should be taken by the controller to correct data inaccuracy factors and limit the risks of errors inherent in profiling.

3.10. The controller should periodically and within a reasonable time reevaluate the quality of the data and of the statistical inferences used.

C. Sensitive data

3.11. The collection and processing of sensitive data in the context of profiling is prohibited except if these data are necessary for the lawful and specific purposes of processing and as long as domestic law provides appropriate safeguards. When consent is required it shall be explicit where the processing concerns sensitive data.

4. Information

4.1. Where personal data are collected in the context of profiling, the controller should provide the data subjects with the following information:

- a. that their data will be used in the context of profiling;
- b. the purposes for which the profiling is carried out;
- c. the categories of personal data used;
- d. the identity of the controller and, if necessary, her or his representative;
- e. the existence of appropriate safeguards;
- f. all information that is necessary for guaranteeing the fairness of recourse to profiling, such as:
 - the categories of persons or bodies to whom or to which the personal data may be communicated, and the purposes for doing so;
 - the possibility, where appropriate, for the data subjects to refuse or withdraw consent and the consequences of withdrawal;
 - the conditions of exercise of the right of access, objection or correction, as well as the right to bring a complaint before the competent authorities;
 - the persons from whom or bodies from which the personal data are or will be collected;
 - the compulsory or optional nature of the reply to the questions used for personal data collection and the consequences for the data subjects of not replying;
 - the duration of storage;
 - the envisaged effects of the attribution of the profile to the data subject.

4.2. Where the personal data are collected from the data subject, the controller should provide the data subject with the information listed in Principle 4.1 at the latest at the time of collection.

4.3. Where personal data are not collected from data subjects, the controller should provide the data subjects with the information listed in Principle 4.1 as soon as the personal data are recorded or, if it is planned to communicate the personal data to a third party, at the latest when the personal data are first communicated.

4.4. Where the personal data are collected without the intent of applying profiling methods and are processed further in the context of profiling, the controller should have to provide the same information as that foreseen under Principle 4.1.

4.5. The provisions under Principles 4.2, 4.3 and 4.4 to inform the data subjects do not apply if:

- a. the data subject has already been informed;
- b. it proves impossible to provide the information or it would involve disproportionate effort;

c. the processing or communication of personal data for profiling is expressly provided for by domestic law.

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

4.6. Information provided to the data subject should be appropriate and adapted to the circumstances.

5. Rights of data subjects

5.1. The data subject who is being, or has been, profiled should be entitled to obtain from the controller, at her or his request, within a reasonable time and in an understandable form, information concerning:

a. her or his personal data;

b. the logic underpinning the processing of her or his personal data and that was used to attribute a profile to her or him, at least in the case of an automated decision;

c. the purposes for which the profiling was carried out and the categories of persons to whom or bodies to which the personal data may be communicated.

5.2. Data subjects should be entitled to secure correction, deletion or blocking of their personal data, as the case may be, where profiling in the course of personal data processing is performed contrary to the provisions of domestic law which enforce the principles set out in this recommendation.

5.3. Unless the law provides for profiling in the context of personal data processing, the data subject should be entitled to object, on compelling legitimate grounds relating to her or his situation, to the use of her or his personal data for profiling. Where there is justified objection, the profiling should no longer involve the use of the personal data of the data subject. Where the purpose of the processing is direct marketing, the data subject does not have to present any justification.

5.4. If there are any grounds for restricting the rights set out in this section in accordance with Section 6, this decision should be communicated to the data subject by any means that allows it to be put on record, with a mention of the legal and factual reasons for such a restriction.

This mention may be omitted when a reason exists which endangers the aim of the restriction. In such cases, information should be given to the data subject on how to challenge this decision before the competent national supervisory authority, a judicial authority or a court.

5.5. Where a person is subject to a decision having legal effects concerning her or him, or significantly affecting her or him, taken on the sole basis of profiling, she or he should be able to object to the decision unless:

a. this is provided for by law, which lays down measures to safeguard data subjects' legitimate interests, particularly by allowing them to put forward their point of view;

b. the decision was taken in the course of the performance of a contract to which the data subject is party or for the implementation of pre-contractual measures taken at the request of the data subject and that measures for safeguarding the legitimate interests of the data subject are in place.

6. Exceptions and restrictions

Where it is necessary in a democratic society for reasons of state security, public safety, the monetary interests of the state or the prevention and suppression of criminal offences, or protecting the data subject or the rights and freedoms of others, member states need not apply the provisions set out in Sections 3, 4 and 5 of the present recommendation, where this is provided for in law.

7. 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.

8. Data security

8.1. Appropriate technical and organisational measures should be taken to ensure the protection of personal data processed in accordance with the provisions of domestic law enforcing the principles set out in this recommendation, to guard against accidental or unlawful destruction and accidental loss, as well as unauthorised access, alteration, communication or any other form of unlawful processing.

These measures should ensure a proper standard of data security having regard to the technical state of the art and also to the sensitive nature of the personal data collected and processed in the context of profiling, and evaluating the potential risks. They should be reviewed periodically and within a reasonable time.

8.2. The controllers should, in accordance with domestic law, lay down appropriate internal regulations with due regard to the relevant principles of this recommendation.

8.3. If necessary, the controllers should appoint an independent person responsible for the security of information systems and data protection, and qualified to give advice on these matters.

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

8.5. Suitable measures should be introduced to guard against any possibility that the anonymous and aggregated statistical results used in profiling may result in the re-identification of the data subjects.

9. Supervisory authorities

9.1. Member states should mandate one or more independent authorities to ensure compliance with the domestic law implementing the principles set out in this recommendation and having, in this respect, the necessary powers of investigation and intervention, in particular the power to hear claims lodged by any individual person.

9.2. Furthermore, in cases of processing that use profiling and entail special risks with regard to the protection of privacy and personal data, member states may foresee either:

- a. that controllers have to notify the supervisory authority in advance of the processing; or
- b. that this processing is subject to prior checking by the supervisory authority.

9.3. The above authorities should inform the public of the application of the legislation implementing the principles set out in this recommendation.