COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 31 August 2010 CDCJ-BU (2010) 15
*[CDCJ/Documents CDCJ-BU 2010/CDCJ-BU (2010)15E]*

**BUREAU**
**OF THE EUROPEAN COMMITTEE ON LEGAL CO-OPERATION**
**(CDCJ-BU)**

# DRAFT RECOMMENDATION ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA IN THE FRAMEWORK OF PROFILING

# AND ITS DRAFT EXPLANATORY MEMORANDUM

Document prepared by the
Directorate General of Human Rights and Legal Affairs

**TABLE OF CONTENTS**

**DRAFT RECOMMENDATION**

**Draft Recommendation CM/Rec(2010)… of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the framework of profiling**

*(Adopted by the Committee of Ministers on … 2010 at the … meeting of the Ministers' Deputies)*

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 ever closer unity among its members;

2. 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 for 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;

3. 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 the data stemming in particular from social networking, video surveillance systems, biometric systems and by 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;

4. 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 data of several individuals. Noting that the development of ICTs enables these operations to be performed at a relatively low investment;

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

6. 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 he/she can reasonably presume to be known to the controller;

7. 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;

8. 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 he or she makes of his or her identity;

9. 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;

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

11. 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 108") and other data, can enable the generation of new sensitive data concerning an identified or identifiable person. Considering that such profiling can expose individuals to particularly high risks of discrimination and attacks on their personal rights and dignity;

12. Considering that the profiling of children may have serious consequences for children throughout their whole 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;

13. 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;

14. 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, 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;

15. Recalling in this regard the general principles on data protection in Convention 108;

16. Recalling that every person must 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, in particular, not adversely affect trade secrets or intellectual property or the copyright protecting the software;

17. 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 No. R (97)18 on the protection of personal data collected and processed for statistical purposes;

18. Taking into account the Council of Europe Convention of Cybercrime (CETS 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;

19. Taking into account both Article 8 of the European Convention of Human Rights, as interpreted by the European Court of Human Rights and new risks created by the use of information and communication technologies;

20. 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;

21. 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 this requires comparable data protection in all the member states of the Council of Europe;

Recommends that the governments of member States:

1. apply the appendix of the present recommendation to the collection and processing of personal data used in the context of profiling;

2. take measures to ensure that the principles set out in the appendix to this recommendation are reflected in their law and practice;

3. 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;

4. 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 to put in place the technologies found in the appendix to this recommendation.

**Appendix to Recommendation CM/Rec …..**

## 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 manpower.

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, namely in order to take decisions concerning him or her; or for analysing or predicting personal preferences, behaviours and attitudes.

f. “Information society service” refers to any service, normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

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, must be guaranteed during the collection and processing of personal data subject to this recommendation.

2.2 Profiling requires transparency and must not lead to discrimination, measures or decisions contrary to the law.

2.3 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 among others 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 Moreover, collection and processing of personal data in the context of profiling may be performed:

a. if it is provided for by law, or

b. if it is permitted by law and

- the data subject or his or her legal representative has given his or her free, specific and informed consent; or
- 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, or
- 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, or
- it 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, or
- if it 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 Chapter 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 service 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 aiming 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 it is expressly provided for by law comprising 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 re-evaluate 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, his or her 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 of 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 or bodies from whom or 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 of not replying for the data subjects;
   - 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 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 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 4.1.

4.5 The obligations under 4.2 and 4.3 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 his or her request, within a reasonable time and in an understandable form, information concerning:

a. his or her personal data;

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

c. the significance and envisaged consequences of the profile attributed to him or her if not prohibited by law;

d. the purpose for which the profiling was carried out and the recipients.

5.2 Data subjects should be entitled to secure, as the case may be, correction, deletion or blocking of their personal data, 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 his or her situation to the use of his or her 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 Chapter in accordance with Chapter 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 him or her or significantly affecting him or her, taken on the sole basis of profiling, he or she 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 viewpoint, or

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 data subject are in place.

**6. Exceptions and Restrictions**

6.1 Member states may decide not to apply the provisions set out in Chapters 3, 4 and 5 of the present recommendation, when such a derogation is provided for by law and 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.

**7. Remedies**

7.1 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 authority 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:

a. either 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.

**DRAFT EXPLANATORY MEMORANDUM**

## I. Foreword

### Privacy as a fundamental right

1. The Council of Europe, which has its headquarters in Strasbourg (France), is the oldest European political organisation. It was established in 1949 and with its 47 member states now covers almost the whole of Europe.

2. One of the first – and also one of the most important – conventions drawn up by the Council of Europe is the Convention for the Protection of Human Rights and Fundamental Freedoms, more commonly known as the European Convention on Human Rights ETS No. 5 (hereinafter "ECHR"), which was opened for signature in 1950. It established the European Court of Human Rights (hereinafter "the Court"), an international court with jurisdiction to rule on applications by individuals or states alleging violations of the civil and political rights enshrined in the ECHR. Its judgments are binding on the respondent states and require governments to amend their legislation or administrative practices in numerous areas.

3. The first paragraph of Article 8 of the ECHR provides that: "Everyone has the right to respect for his private and family life, his home and his correspondence". Paragraph 2 stipulates that this right can only be restricted by a public authority in accordance with domestic law and in so far as is necessary, in a democratic society, to safeguard specific legitimate aims.

4. On these grounds the Court has, in its judgments, held that although measures which interfere with privacy may be designed to protect democracy they should not destroy it in the process[1]. The Court has also developed case law under which Article 8 may also give rise to positive obligations that are inherent in effective "respect" for private life. In accordance with this theory of so-called "positive obligations", the state must take the necessary measures, including legislative measures, to ensure practical and effective compliance with the rights deriving from Article 8 of the ECHR.

5. The protection of personal data therefore plays a fundamental role in the exercise of the right to private or family life enshrined in Article 8, whereby national legislation must provide appropriate safeguards to prevent any use of personal data which does not comply with the guarantees provided for in this article and to ensure the effective protection of registered personal data against misuse and abuse[2].

6. The ECHR also preserves, in Article 10, the fundamental right to freedom of expression. The right to freedom of expression explicitly includes the "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers". The freedom to receive information is considered as including the "freedom to seek information". The exercise of this freedom to receive, impart or seek information with the help of information and communication technologies implies anonymity since, without such a reasonable safeguard, the fear of interference by the public authorities or private companies would be legitimate, even if this interference was no more than the observation and recording of the behaviour of Internet users.

---

[1] ECHR (Plenary) judgment of 2 August 1984 *, Malone v. the United Kingdom*, No.. 8691/79 Series A par. 82 .

[2] Furthermore, in the Charter of the fundamental rights of the European Union, the right to the protection of personal data is a separate right alongside the right to the right to respect for his or her private and family life.

**Convention 108 and its Additional Protocol**

7. In the years following the adoption of the ECHR, it became increasingly necessary to develop more specific and systematic legal protection of privacy to ensure the effectiveness of such protection and deal with the growing number of new dangers of violation of the right to privacy resulting from the use of information technologies.

8. This led to the drafting of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108)[3], known as "Convention 108" at the same time as the Organisation for Economic Co-operation and Development (OECD) was drafting its "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data". Non-member states of the Council of Europe, such as Australia, Canada, Japan and the United States of America, helped draft Convention 108[4].

9. This Convention was opened for signature on 28 January 1981. To date it has been ratified by 41 member states of the Council of Europe; others have signed it and are preparing to ratify it.

10. It is a binding legal instrument with a universal scope as the Committee of Ministers of the Council of Europe agreed to consider requests for accession from states which are not members of the organisation.[5]

11. On 15 June 1999, the Committee of Ministers adopted amendments to Convention 108 to allow the accession of the European Communities[6].

12. Convention 108 establishes principles applicable to both the public and the private sector concerning the quality of data, the processing of sensitive data, the need to inform the person concerned and the right of access and rectification.

13. It provides for the free flow of personal data between the Parties to the Convention. This free flow may not be obstructed purely for personal data protection reasons. The aim of this provision is, and continues to be, to enable the transfer of personal data within the geographical limits of countries which offer an adequate level of protection.

14. The existing safeguards have been reinforced by an Additional Protocol[7] requiring that Parties set up one or more supervisory authorities exercising their functions in complete independence and that they should not, in principle, allow the transfer of data to countries or organisations which do not provide an adequate level of protection. It is therefore possible to refuse to transfer data to a country which does not provide adequate protection or to a country which is not party to Convention 108[8].

**The Council of Europe's standard-setting activities in the field of data protection**

15. Although the provisions of Convention 108 have today been incorporated into the domestic law of most Council of Europe member states, the complexity of issues concerning the effective protection of personal data, caused in particular by the constant emergence of new technologies and practices, calls for innovative solutions and analysis. In view of these challenges, the national data protection authorities and data protection commissioners are at the forefront of efforts to address these

[3] See http://www.coe.int/dataprotection
[4] Explanatory Memorandum to Convention 108, § 15.
[5] CM(2008)81.
[6] CM(98)182.
[7] Additional Protocol to the Convention 108, regarding supervisory authorities and transborder data flows (ETS No. 181).
[8] Additional Protocol, Article 2.

complex issues and find appropriate solutions. Courts also provide individuals with protection when faced with violations of their privacy.

16. The Committee of Ministers has adopted several recommendations on the basis of Convention 108.[9] The aim is to ensure that the collection and processing of data in a given sector (banking, insurance, health, police etc.) or carried out with the help of a particular technique or technology (for example smart cards, video surveillance or direct marketing) or relating to a particular category of data (sensitive, biometric, etc.) are carried out in accordance with the general principles established by Convention 108.

17. These recommendations are addressed to the governments of all Council of Europe member states. Although they are not legally binding, they constitute standards of reference and a request to consider the possibility of enacting and applying domestic law in conformity with the principles set out in the recommendations.

18. While the absolute need for legislation continues to be recognised, self-regulation should also encouraged among information society players to ensure that privacy and the protection of data are respected more effectively in the face of vast networks of telecommunications which know no boundaries, the growing flow of personal data and the steady development of information and communication technologies.

**The Council of Europe's work on profiling**

19. In 2008, a team of experts presented a report on the application of Convention 108 to the process of profiling[10] at the 24th plenary meeting of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD).

20. The report highlighted, in particular, the use of numerous technologies, such as web bugs and cookies, which may be used in combination and which, by their very nature, make it possible to observe and trace individuals without their knowledge, not only by the sites they have visited but also by other companies established outside member states of the Council of Europe. The report also showed that these practices, which are widespread but little known to the general public, could constitute a breach of the right to privacy of the persons concerned.

21. The presentation of the report was followed by a discussion within the T-PD, in particular on the conclusions of the report, which called for the drafting of a new recommendation in this field. At its 1050th meeting on 13 March 2009, the Committee of Ministers considered the opportunity of carrying out work in this field and instructed the European Committee on Legal Co-operation (CDCJ) to prepare a recommendation on profiling in close co-operation with the T-PD[11]. The draft recommendation on the protection of individuals with regard to the automatic processing of personal data in the framework of profiling was drawn up on the basis of this decision.

22. A public consultation was held on the draft recommendation and comments were sought from various stakeholders such as Internet access providers, associations of online advertisers and representatives of trade and consumers' associations. The European Commission, the International Chamber of Commerce and the French speaking association of the data protection authorities among others also contributed to the work with their expertise.

23. The text was transmitted to the CDCJ, which approved it at its 85th plenary meeting (11-14 October 2010) and then transmitted it to the Committee of Ministers for adoption.

---

[9] http://www.coe.int/t/dghl/standardsetting/dataprotection/Legal_instruments_en.asp
[10] http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profiling_2008_en.pdf
[11] CM/Del/Dec(2009)1050/10.6E / 13 March 2009.

24. Finally it should be mentioned that, once adopted, the recommendation on the protection of individuals with regard to the automatic processing of personal data in the framework of profiling will be the first international legal instrument laying down a set of principles for possible general application to all forms of personal data processing using profiling techniques.

## II. Introduction

25. The concept of the World Wide Web emerged in the early 1990s and developed exponentially all over the world. The web gradually linked institutions and individuals via web servers. At the same time, the Internet linked individuals with one another, initially via e-mail and subsequently via blogs and, more recently, social networks, commonly designated Web 2.0 or the participatory web.

26. A new stage in the technical development of the global telecommunications networks is already in sight. This will involve not just interlinking individuals but also endowing the objects that surround them firstly with software intelligence and secondly with the capacity to communicate over a local network linked to the Internet. The initial applications of “Radio Frequency Identification” (RFID) technology foreshadow the possible future world of so-called "ambient intelligence".

27. The Internet of the future will therefore not just connect human beings with one another but will also interlink smart devices (Internet of things) that surround people in their everyday lives and support them as they move around and carry out their everyday activities. In this world of ambient intelligence, objects will constantly monitor and analyse, probably without their knowledge, the behaviour of the human beings around them, so as to interact with them in a dynamic way.

28. One could imagine that the television linked to the Internet will be able to inform the refrigerator of the date when a football match is next being screened. The refrigerator will then order the necessary number of cans of beer based on the quantity of beer consumed the last time a football match was on television. The intelligent washing machine will use RFID chips embedded in clothing to sort the laundry and select the right wash programmes for the different kinds of textiles. A pacemaker will probably be able to call the emergency services if the wearer shows the initial signs of a heart attack and to instantaneously transmit the patient's location and full medical data.

29. In parallel, this development is being accompanied by the significant growth in data storage, processing and communication capacities makes the gathering of information on more or less broad population groups in huge databases and the correlation on a random or non-random basis possible, and allows the construction of group "profiles" that can be applied to classify individuals by identifying them with given profiles and to "statistically" predict their future behaviour. For instance, the analysis of data on the purchases in the basket of a supermarket customer who shops at a given time in a given neighbourhood makes it possible to identify this basket as belonging to a given consumer profile; and therefore concludes that it is someone who should in principle be interested in a given product or service offer.

30. The gradual emergence of a smart things society, in which these devices will in the long run be connected to the Internet and coupled with many techniques (such as cookies, web bugs, etc.) that are in general use on sites consulted by large numbers of users worldwide will accentuate the profiling and make the recourse to it a permanent occurrence. This close knowledge of individuals, attaining a hitherto unknown magnitude, ubiquity and effectiveness, would make it possible not only to try to sell them products on the basis of their profiles but also to adapt the prices of goods or services in a dynamic way in line with the elasticity of the individual consumer's demand.

31. This network development raises a number of concerns. The manifold uses of the technologies described unquestionably offer considerable benefits for the individuals concerned, but they also engender not insignificant risks of abuse and infringements of fundamental rights and freedoms.

Indeed, a number of organisations, some of which already have a strong foothold in the information and communication society, could use the resulting information in their own interests, without the data subjects being aware of this or being offered any form of fair recompense. Special safeguards need to be developed in order that the rewards of the new information and communication society do not undermine the fundamental rights and freedoms of the same society. The provision of further information outlining the main features of the technologies would allow for their optimal use and at the same time a better protection of data subjects' rights. E-inclusion and e-literacy should also play an important role.

32. Nowadays, recent technical developments make it possible, notably through automatic analysis of trajectories and eye reactions, to measure individuals' emotional responses and focuses of interest, even without them being aware of it. Experiments currently being carried out show that the marketing sector is interested in this new technique for gauging emotions in real time.

33. The risks of health insurance companies using health data to determine particular costs and above all to exclude certain people from benefiting from some offers should also be highlighted. Such individualisation of file processing alters the very idea of insurance, which implies a certain risk pooling.

34. Apart from direct marketing uses, profiling techniques could be increasingly developed and used in other contexts relating to public interest often without being publicised or having been put through any form of control or safeguard.

35. It is possible, for example, to imagine the advantages for a political party, an association or a group of activists of being able to profile individual voters in such a detailed way and possibly to adapt, in real time, the on-screen presentation of its political manifesto to a given profile. It would also be technically feasible for a government or a group of activists to make mass use of profiling of telecommunications network users, including on private networks, to identify the most subversive individuals and take steps that discriminate against or exclude them.

36. In the public sector the possibility of correlating information originating from a number of databases using unique identifiers similarly makes it possible to pinpoint, in principle, potential social benefit recipients and fraud suspects and may be of assistance in identifying the perpetrators of offences. Without doubt, this identification is legitimate if it is accompanied by sufficient safeguards allowing each person to challenge the 'truths' coming out from the computer.

37. Beyond these applications in the public or private sectors, a few additional major issues should be noted as a result of this increasingly vast collection and of the finer profiling it induces. Firstly, the important volume of information specifically pertaining to individuals collected by intelligent devices will make possible to identify, track and geolocate any person at any moment. In these circumstances preserving anonymity or rather the possible non-application of a profile is already increasingly difficult, if not impossible, from a technical standpoint. Secondly, it would also be possible by comparing and matching in theory harmless information on individuals transmitted over the networks to deduce, with a slight margin of error, certain sensitive data relating, for instance, to their health, religion, sexual preferences or trade union membership.

### II.1 Profiling Characteristics

38. Profiling, as understood in the context of this recommendation, takes place in three technically distinct stages:

- A stage during which digitised **observations** regarding individuals' behaviour or characteristics are collected and stored on a large scale (data-warehousing). The resulting data may be nominative, coded or anonymous.

- A stage during which these data are analysed and "probed" (data-mining) permitting the determination of **correlations** between different behaviours/characteristics and other behaviours/characteristics.
- An **inference** stage during which, on the basis of certain observable behavioural variables or characteristics specific to a, generally identified, individual, new past, present or future characteristics or behavioural variables are deduced.

39. It should be noted that the first two stages (data-warehousing and data-mining) can be carried out using anonymised or coded data. Where anonymised data are used, it is technically impossible to identify the individual concerned by the observations. If coded data are used, a trusted third party is able to identify the individual by decoding the data. The possibility, even in theory, that "anonymous" data could be de-anonymised in fact means that the data are not anonymised in an effective way.

40. As a general rule the third stage concerns an individual who is identified or identifiable and is carried out as described above, in a growing variety of fields and by increasing numbers of actors.

41. It is doubtless important to distinguish profiling techniques from other aids to decision-making. Selecting individuals on the basis of their real characteristics does not constitute profiling. For example, if a bank selects rich customers earning over 10,000 Euros per month and with assets of at least one million Euros, this is an objective selection process, which, unlike profiling, does not involve a margin of error. From a technical standpoint, this kind of selection simply entails requesting information from a Structured Query Language (SQL) server and does not require data-mining. Although the bank may employ the familiar term "rich customer profile", this type of profiling, which in fact involves selecting individuals on the basis of accurate data specific to them, does not qualify as profiling within the meaning of this recommendation. In the context of this recommendation, profiling requires a process of statistical extrapolation producing partially accurate, and therefore also partially inaccurate, results.

42. Concerning profiling in the bank sector, it is used to make an assessment of future or existing customers' risks (credit scoring). In this context, it is a matter of analysing thousands or millions of good and bad payers' histories so as to be able to identify the individual characteristics that correlate with the capacity or failure to repay a loan. When signing a loan contract, the bank will ask the prospective borrower a number of apparently neutral questions on the basis of which it is possible to calculate the probability that a given individual will or will not duly honour a loan. It is clear that, in the specific case of credit scoring, attributing the characteristic of "good" or "bad" payer to an individual always involves some margin of error. Nonetheless, the use of this kind of profiling will enable a bank to reduce, on average, its risk of assigning a wrong credit rating. This profiling involves a small risk of two kinds of error (extending a loan to a person who will fail to repay and refusing a loan to a person who would have repaid). However, such errors are devoid of detrimental financial consequences for the bank as long as they remain marginal. In other words, the use of profiling can offer overall advantages for businesses, governments and various other institutions but generates errors in the case of a minority of the profiled individuals and thus requires a certain number of precautions.

43. Another example of profiling is that performed for medical research purposes and to detect congenital diseases. By analysing the genetic data of thousands or millions of patients and data relating to a given congenital disease, data-mining systems can establish correlations between the presence or absence of certain genetic characteristics and a specific disease, again with some margin of error. This makes it possible to deduce that a patient with certain genetic characteristics has a likelihood of developing this disease. Subjects at risk can thus be identified and encouraged to take preventive measures to reduce the disease's occurrence - or they can be charged higher insurance premiums for example.

44. In the field of taxation, public authorities already use profiling techniques to identify taxpayers who are more likely than others to evade tax by fraudulent means. It would be legitimate for the state to carry out targeted checks on the basis of profiling, it being understood that an unfavourable profile can not amount to a presumption of fraud, but simply guide the authorities in their investigations. .

45. In the commercial field, profiling can tailor the price of goods or a service according to a consumer. It is indeed technically feasible to adapt the price of goods or a service according to a consumer's profile. This risk is multiplied on the Internet in so far as the price for goods or a service is displayed in differing locations (on consumers' individual screens), unlike in shops where the price ticket is the same for all customers. Adapting prices according to a customer's profile constitutes processing of the customer's data and customer profiling must therefore be performed in accordance with the principles of Convention 108. Making use of the argument that the current technological context is reducing this risk would in fact jeopardise the principle of technological neutrality which is underpinned in the recommendation.

### II.2 How to apply the principles of Convention 108 to profiling activities

46. The above examples clearly show that if the rapid development and use of profiling techniques entail new risks for individuals, some protection measures must be reinforced and detailed so as to maintain the level of protection of freedoms and privacy recommended by the Council of Europe in 1981.

47. Profiling is never a purpose under the terms of Article 5 of Convention 108, but, like automation, it constitutes a technical process that a data controller can use to facilitate attainment of a given goal. In the above examples the bank's purpose is to manage credit risk, the medical researcher's purpose is to prevent genetic diseases and the government's purpose is to combat tax evasion.

48. Profiling is a specific personal data processing method allowing the data controller to reach a goal. However, the use of a profiling technique in principle inherently entails a number of significant risks, as set out below.

### II.3 Profiling risks

#### Lack of transparency in processing and of the data processed

49. As a general rule, in the case of data processing without profiling the personal data are factually accurate and relate to identified or identifiable individuals. In this context, data subjects are generally aware of, or can guess, the nature of the information the data controller holds concerning them. Since profiling generates new data for an individual based on data relating to other persons, the data subject in principle cannot suspect the existence of correlation processes that might result in certain characteristics of other individuals being attributed to him or her on the basis of a probability calculation.

50. For instance, a bank customer who has defaulted on a loan can rightly expect that the bank will refuse to give him or her another loan or will ask for specific guarantees. Conversely, bank customers who have never had any repayment problem, or have never even been granted a loan, in principle could not imagine that the bank, having asked them a number of apparently harmless questions, would use, via profiling techniques, the replies to assign them to a creditworthiness category to which, strictly speaking, they do not belong.

51. Data processing involving the use of profiling is in principle intrinsically far less transparent for data subjects than other personal data processing. Therefore the controller must provide the data subject with more easy to understand information when profiling is being used and the right of access must

be reinforced, both as regards the fact that his or her data is used in the course of profiling and the fact that the profile is being applied to him or her.

**Binding application of other people's data**

52. This way of attributing to a given individual "personal" data which in fact belong to other people creates a novel situation. Individuals are in practice answerable for their own actions and are held socially and legally responsible for them. The effect of profiling is the attribution - and even binding application - to individuals of personal data pertaining to other individuals unknown to them, with whom they merely share a number of characteristics. If processing involving profiling has a predictive purpose it will entail attributing to an identified or identifiable individual the behavioural characteristics of a group having some shared characteristics with that individual so as to deduce *brand new* characteristics for the individual concerned. This is one of the features of profiling: it could create new personal data from data relating to a group.

**Inevitable uncertainty**

53. Since profiling is based on the use of statistics, there is a real likelihood that a given characteristic will be wrongly attributed to an identifiable or identified individual. For example, predictive data relating to an individual which have been extrapolated from data concerning the previous behaviour of a group cannot always be accurate. It is generally possible to calculate the rate of occurrence of two kinds of error (firstly the probability of wrongly assigning a person to a category and secondly that of excluding from a category those who in fact belong to it). In the case of credit scoring, use of profiling will result, normally to a minor extent but nonetheless inevitably, in loans being extended to individuals who will not honour them and refused to individuals who would have repaid. In the fight against terrorism, the use of black lists based on statistical inferences is bound to result in non-terrorists being prevented from boarding a plane and offers no absolute guarantee that terrorist passengers will be intercepted. Such examples, while not calling into question the legitimacy of the purposes of profiling, however, demonstrate the need to adopt certain safeguards.

54. In practice, use of profiling techniques jeopardises - usually to a minor extent albeit inevitably - data accuracy, as required by Article 5d of Convention 108. Profiling should respect the principle of accuracy of data. To curtail the risk that inaccurate data is bindingly applied to an individual, it is necessary, particularly in the most sensitive areas, to reinforce the data subject's right of access not only concerning his or her own data, but also with regard to the logic of the processing being or having been carried out using the data. Since profiling entails a risk that the data subject may be attributed inaccurate data, the right of objection must also be reinforced.

55. The data controller will also be required to exercise special diligence so as to ensure that the data used at the first two stages (data-warehousing and data-mining) are accurate and up-to-date, without regard to the fact that these data may concern identified or identifiable data subjects. The data-mining algorithms must be devised and tested in accordance with the rules of the art so as to minimise the risk of occurrence of the two kinds of error above. In some cases use of anonymous accurate data is to be recommended. In such cases, the requirements governing the processing of anonymous data could *prima facie* seem to constitute an extension of the scope of Convention 108. Profiling results in the creation of new personal data from anonymous data : both the warehoused data (which may be anonymous) that constitute the raw material and the process whereby the new data are created must be designed, and possibly adapted, so that the end result of the profiling process is personal data that are as accurate as possible, in accordance with Article 5d of Convention 108. Since the quality of these two basic ingredients at the end of the profiling process is clearly of key importance in maximising the accuracy of the personal data generated, Article 5d mentioned above requires that all reasonable precautions should be taken to guarantee the quality of these ingredients.

56. For example, if an insurance company adapts car insurance premiums on the basis of vehicle thefts in the insured person's neighbourhood, it can legitimately be required to use recent, up-to-date statistics and a recent, secure analysis programme, notwithstanding the full anonymisation of the data concerning vehicle thefts. A last argument to be borne in mind is that, of the three stages involved in profiling, even though the first two stages may use anonymous data, the third results in application of the outcome to identified or identifiable individuals. In so far as the three stages are inseparable, they must all be considered part of personal data processing, as explained in the expert report on which this recommendation is based.

57. Lastly, the risks involved in data processing involving the use of profiling must, in certain sensitive matters, be quite simply prohibited or made subject to specific requirements. Indeed, although it is in general acceptable that data subjects should be able to rely on the rights of access and of objection where profiling is used in the processing of relatively insensitive data, we cannot condition access to essential goods and services, such as housing or employment, by the sole - sometimes erroneous - outcome of processing involving profiling. Each member state will doubtless have to take a position on this issue, according to the context and the guarantees offered by a proposed profiling system.

**Data decontextualisation**

58. As mentioned in the expert report, the obligation to respect the right of one's privacy implies that data controllers should only process data pertaining to a sphere of the private life of the individual concerned. It is intended to guarantee a hermetic seal between individuals' different spheres of life and that data are used solely for the stated purpose.

59. Thus, the banker who wants to evaluate the credit of someone does not have to worry about the social relations of his or her client. In other terms, only the data relating to the sphere of life affected by the purpose of processing should be taken into consideration.

60. This division of private life into hermetically sealed spheres unfortunately has no technical equivalent. Very often the data subject will have the same identifiers (typically surname, first name, date of birth and address) in each sphere. It is technically possible for profiling techniques to be used to process data collected in different "spheres" of an individual's private life. The implementation of data-mining techniques, as described above, then makes it possible to determine statistical correlations between behavioural characteristics belonging to separate spheres of private life. This would make it possible, for example, through large-scale analysis of anonymous individuals' purchases and of characteristics relating to sexual behaviour to identify correlations between purchasing habits and an individual's heterosexuality or homosexuality. This correlation could then logically be used in the opposite sense: on the basis of a purchasing profile it would become theoretically possible to presume, with some - generally quantifiable - margin of error, that an identified or identifiable individual is heterosexual or homosexual. This is to say that profiling can be used to extrapolate deduction rules from non-sensitive data to sensitive data, with a reasonable range of certainty.

61. This risk of cross-matching data pertaining to separate spheres of private life is increased where the profiling is based on data obtained from an individual's Internet use. This is because, by nature, a computer or telecommunications terminal is not used solely in a given sphere of life but will habitually be utilised by an individual for all kinds of purposes. Typically, individuals tend to use the same terminal to communicate with their family, employer, friends, doctor, trade union, bank or lover. This means that, in practice, where a general search engine is used, the service provider hosting the search engine has a "global" view of an identified individual[12]. In other words, the

[12] If only temporarily via a static IP address and possibly in the longer term via a fixed IPv4 address or a dynamic IPv6 address incorporating the network interface card's Media Access Control (MAC) address, namely an identifier, or even via a residual cookie.

terminal nowadays plays a key, even vital, technical role in collecting network users' telecommunications data.

62. The terminal equipment has now become a tool, a place, the utilisation of which generates a large number of behavioural data and starting from which many kinds of personal data processing relating to the same data subject are performed concerning spheres of the individual's private life that must remain technically separate from one another. That is why, the recommendation emphasises the need to regulate the functioning of terminals, and in particular web browsers, and to prohibit software aiming at monitoring terminal or communication network use unless it is provided for by domestic law comprising appropriate safeguards.[13]

63. The principles of the proportionality and fairness of processing also justify the restrictions imposed on the collection of data not linked to the purpose of the processing.

## III. Comments on the provisions of the recommendation

### III.1 Preamble

64. The preamble sets out the reasons that have led the Committee of Ministers to present the recommendation to governments of member states.

65. In the context of this recommendation, the Committee of Ministers notes that the continuous development of new information and communication technologies (volume of data stored and transmitted, computing speeds and sophisticated processing algorithms) now makes it possible, firstly, to collect and process various types of personal data relating to many individuals and, secondly, to make connections between these data for profiling purposes.

66. The Committee of Ministers observes that while the many uses of these new technologies undoubtedly provide considerable benefits for the data subjects, they nevertheless create radically new and by no means insignificant risks of abuse and infringement of fundamental rights and freedoms since profiling is often used without the knowledge of the individuals concerned and may therefore undermine the fairness of data processing in so far as the data subjects are unaware of the existence or logic of their profiling. In this case, they cannot understand the logic underpinning the processing or exercise a right of access or objection.

67. The Committee of Ministers recognises the importance, where profiling techniques are concerned, of encouraging and guaranteeing the protection of personal data, especially the sensitive data referred to in Article 6 of Convention 108.

68. The Committee of Ministers has defined the purpose of this recommendation as being to establish appropriate procedures to guarantee that personal data for profiling are collected and processed with due regard for individuals' fundamental rights and freedoms and in particular that this collection and processing ensure an appropriate balance between use of profiling and the right to privacy. This initiative of the Committee of Ministers has become necessary against a background of personal mobility and market globalisation, requiring equivalent protection of individuals in all Council of Europe member states.

[13] Article 5 of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

69. This recommendation will apply without prejudice to other legal standards. In particular, Article 8 of the ECHR secures individuals' right to privacy, whether or not these individuals are identifiable, and the Convention on Cybercrime (CETS No. 185) prohibits unauthorised access to a computer system, whether this system consists of a company server or the terminal of an identifiable or non-identifiable user.

### III.2 Body of the recommendation

70. The question of the recommendation's scope arose during its drafting. The solution of limiting the scope to collection and processing of personal data for profiling purposes solely in the private sector was immediately ruled out. Firstly, such a distinction would have raised difficulties in delimiting the concepts of the private and the public sectors in a society where public authorities are increasingly delegating the tasks originally conferred on them to private companies. An example is a private company given responsibility for the transfer of prisoners which has recourse to profiling techniques.

71. Secondly, regulating profiling in the private sector alone would have been discriminatory, creating a distortion of competition among entities participating in or using profiling. This distinction would also have weakened the protection of data subjects, since profiling is often used for the award of entitlements or benefits. It goes without saying that, although profiling in the public sector can often have clear grounds of legitimacy (combating tax or benefit fraud, identifying potential recipients of specific forms of assistance, and so on), it entails significant risks since such profiling can target broad categories of the population, lead to decisions having a major impact on individuals who are profiled negatively and be based on a wealth of data obtained from all public administrative departments.

72. Thirdly, no distinction between the private and the public sectors is drawn in Convention 108, in particular because these terms may have different meanings in different countries and depend on the specific rules applied to a given activity sector by the state. Moreover, following the recent entry into force of the Treaty of Lisbon it would seem that this distinction is being abandoned in Community law.

73. So governments of member states are encouraged to apply principles contained in the appendix to the recommendation to all kinds of collection and processing of personal data used for profiling purposes.

74. However, drawing on other legal instruments of the Council of Europe, the possibility of a derogation was established. Under Chapter 6 states may decide not to apply the provisions of Chapters 3, 4 and 5 for reasons linked to public safety, to the prevention and suppression of criminal offences (combating crime in general; intelligence-related activities, and so on) or to the state's monetary interests, which is notably the case of measures to combat tax or benefit fraud. Since this possibility of exception is based on Article 9 of Convention 108, the grounds for derogations mentioned in the present recommendation are construed in the same way as those cited in Article 9.

75. Principle 6.1 nonetheless stipulates, in accordance with Article 8.2 of the ECHR, that derogations must be provided for by law and constitute a measure necessary in a democratic society. The Court has developed a considerable body of case law that can be of assistance in interpreting and applying this principle (in particular regarding definitions stated by the law and of a measure necessary in a democratic society).

76. In addition, it is recommended that governments of member states take measures to ensure that the principles set out in the appendix are reflected in their legislation and practice.

77. Governments are also encouraged to disseminate the contents of the appendix to the recommendation widely among persons, public authorities and public or private bodies, particularly

those which participate in and use profiling such as data-protection bodies, consumer protection associations or associations promoting civil liberties and standardisation agencies.

78. They are urged, where profiling operations are concerned, to define and promote codes of conduct to ensure that privacy is respected, for example by developing technologies based on the appendix to this recommendation.

### III.3 Appendix to the recommendation

#### 1. Definitions

79. Section 1 lays down definitions for some of the recommendation's key concepts.

80. The terms 'controller' and 'processor' have already been defined in other explanatory memoranda to sector-specific recommendations adopted by the Committee of Ministers[14] in the field of data protection and do not need, according to the authors, further explanation in the framework of this recommendation.

81. **Personal data:** this definition, which has already been used in other recommendations, is consistent with that of Convention 108 as explained in the latter's explanatory report. It has already been used in many recommendations. However, the authors considered it necessary to give a clearer definition, taking into account the particular issue of profiling.

82. Convention 108 limits its scope to personal data alone, since this type of data, unlike anonymous data, technically enables controllers to use an identifier as an access key for every identified or identifiable individual in other processing of personal data.

83. For example, the indication of an individual's civil identity (surname, forename, address) on a till receipt would allow a supermarket to access external data sources (directories, search engines, online mapping services) and find out other information relating to the customer. In today's circumstances, however, the concept of identity cannot be confined to name and address alone. The unique identifier issued automatically to its customers or virtual visitors by a business, a group of businesses or an operator also makes it possible for such searches to be carried out and these connections made. For example, just a customer number would technically enable a supermarket to ascertain, with respect to a particular customer, not only the content of that customer's shopping basket today but also the entire history of that person's previous purchases and even, if the card has an RFID chip, a history of that customer's movements around the shop. In the context of profiling, many individual characteristics go to make up an individual's behaviour. In so far as these characteristics are numerous and specific, it is possible to identify each individual on the basis of behaviour peculiar to that person. As far as profiling is concerned, an individual is genuinely anonymous only if the data values collected for that individual are not unique – in other words, if two different individuals in a given context have the same characteristics. For example, among a crowd of customers, the characteristics "wearing sun glasses and a yellow hat" will not permit a particular individual to be identified if, and only if, in this crowd there are two different people each one wearing sun glasses and a yellow hat.

84. Furthermore, in view of sociological, psychological or even philosophical considerations, it may be asked whether the combination of an individual's multiple behavioural characteristics does not constitute his or her identity. The definition of 'personal data' in European Directive 95/46/EC suggests as much by considering an identifiable person to be one who can be identified, in particular

[14] Explanatory memorandum to Recommendation No. R (2002) 9 of the Committee of Ministers to member states on the protection of personal data collected and processed for insurance purposes and Recommendation No R (97) 18 concerning the protection of personal data collected and processed for statistical purposes.

by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. Is it not the combination of a significant number of individual characteristics that (in the usual sense) identifies an individual, even if that individual shares these characteristics with others? For the purposes of this recommendation, however, we shall consider data to be personal data if an individual's characteristics, whatever their nature (physical, physiological, cultural, economic or social), are unique in the data processing in question.

85. **Sensitive data**: the definition reiterates the list set out in Article 6 of the convention. However, in accordance with Article 11, other categories - such as data on trade union membership or on income - may be defined as sensitive under domestic law. Moreover, data not expressly defined as sensitive may be regarded as such if they are nonetheless accorded a high level of protection by a state

86. **Identifiable person**: a person is said to be identifiable when he or she can be identified through the use of available means whether or not such use involves the services of a third party. Conversely, data are anonymous if identification is possible only through the use of unreasonable manpower[15].

87. **Unreasonable manpower:** means the manpower required from the data controller or any other third party for extremely long, costly and complex operations as compared with their normal activities. It relates, for example, to the technology available to identify data and penetrate their anonymity. Thus, given the rapid progress of IT methods and technology, the time and manpower today considered 'unreasonable' to identify a person may no longer be so in future.

88. **Processing:** article 2c of Convention 108 specifies that the term 'automatic processing' shall include the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.

89. Paragraph 31 of the explanatory report to Convention 108 explains that "in view of the rapid development of data processing technology it was found advisable to formulate a fairly general definition of 'automatic data processing', capable of flexible interpretation". This definition has indeed demonstrated over the years that it is flexible and able to be applied to new situations and technologies. Accordingly, it might be advisable to highlight some of these new situations and show how they come under the definition of automatic processing and thus, in as much as the other conditions for application of Convention 108 are met, under the scope of the Convention.

90. **Collection:** although the concept of personal data collection is not referred to in the definition of automatic processing in Article 2c of Convention 108, it is mentioned in connection with processing in a number of later recommendations. Consequently, this reasserts that the concept of automatic processing must be interpreted as including the concept of collection with a view to automatic processing.

91. This interpretation will apply whatever the method of collection: data may be collected either automatically or manually, the essential point being that automatic processing operations are subsequently applied to these data. Similarly, collection by means of technology such as webcams or mobile phones, in as much as it is connected with other processing operations within the meaning of Article 2c of Convention 108, is included in the concept of automatic processing for the purposes of the Convention.

[15] See also § 26 (b) of the explanatory memorandum to Recommendation No. R (2002) 9 of the Committee of Ministers to member states on the protection of personal data collected and processed for insurance purposes.

92. **Communication:** this term covers every type of data provision to third parties, in particular transmission, dissemination and interconnection. It may be an active provision in response to an individual or global request from a third party. It may also be a passive provision through permission given to a third party to access personal data online. [16]

93. It was decided to keep the explicit reference to this concept in the text of the recommendation since it would clarify the meaning of certain principles (i.e. obligation to give information at the collection stage).

94. **Profile**: a profile is the set of characteristics specific to a group of individuals and, consequently, to each individual belonging to the group. Thus a stay-at-home parent's shopping basket, the geolocation data of persons attending a football match and the bank transactions of an aggressive stock-market investor are characteristic in the sense that they are specific to the groups of individuals analysed. The typical stay-at-home parent's shopping basket will not be the same as a student's; the movements of a football supporter will not be the same as those of someone travelling to work, and the bank transactions of a stock-market speculator will not tally with the profile of a 'family orientated' investor who does not speculate on the stock exchange. Profiling consists of applying to a particular individual the profile of a group with which he or she can be identified through the data collected on him or her. This operation will have the effect of creating new characteristics relating to the identified or identifiable individual profiled in this way. Thus, by examining the shopping basket, it would be possible to identify a stay-at-home parent with two young children who is fond of chocolate; from the geolocation data we can establish that the individual supports a particular football club and is willing to travel long distances to follow his or her team; and by analysing the bank transactions, it would be possible to assign an individual risk profile to an investor. Profiling therefore creates new personal data. Like automation or decision-making assistance systems, profiling is not a purpose within the meaning of Convention 108 but rather a technical procedure that can be used for a purpose, which may be, depending on the case and purely by way of example, the fight against fraud, marketing or worker recruitment.

95. **Profiling:** profiling consists of three stages. The **first** stage consists of large-scale collection of data on individual behaviour. This may be a shopping basket, a telecommunications bill, a list of underground journeys, etc. Data on individual behaviour can be depersonalised or coded.

96. During the **second** stage, these data derived from individual observations undergo computer analysis to correlate certain behavioural characteristics. With statistical tools and algorithms, it thus becomes possible to identify connections between certain kinds of behaviour. Neither human common sense nor human logic plays any part in establishing these correlations. It is purely the computing power of the computer and the sophistication of the algorithms that bring to light correlations often invisible to the naked eye or beyond human reason, albeit without explaining them. For example, what link can be made on the face of it between chocolate consumption, residence in a particular housing estate and the ability to repay a loan? In addition, statistical methods are used to determine a probability factor for the correlation made.

97. In the **third** stage, the correlation thus established is applied to an identified or identifiable individual in order, with a certain margin of error, to deduce some of his or her past, present or future characteristics. However, there is always some risk of error with this application, thus warranting the recommendation. As explained above in the introduction, an individual may be assigned certain present or future characteristics which he or she does not possess and which do not form part of his or her personal history but are those of a group to which he or she is considered more or less likely to belong.

[16] If the communication implies transborder data flow additional provisions would be required.

98. This document wishes to respond to the objection raised that the recommendation goes beyond the scope of Convention 108 in so far as it covers or rather could cover at least in stages 1 and 2 the processing of non-personal data, i.e. anonymous data. As explained in the introduction, in connection with this objection, it was intended that this recommendation should cover, even if only incidentally, the collection and processing of anonymous data in as much as the processing of these data in the first and second stages may be crucial in determining the legitimacy and security of processing in the third stage and that the three stages in reality constitute a continuous process. Thus, for example, it would seem unnecessary to require controllers to use anonymous data that are accurate, genuine and up to date during the first data-warehousing stage, especially as, at first sight and in principle, Convention 108 does not cover anonymous data. In point of fact, the actual substance of these anonymous data can to some extent, as a result of profiling, be found, subsequently and unexpectedly, in the profile of an identified or identifiable person.

99. **Information society services :** this definition corresponds to the one given in the Council of Europe Convention on Information and Legal co-operation concerning "Information Society Services" (CETS 180) and Directive 98/48/EC on regulatory transparency, in force in member states of the European Union.

100. For the purposes of this definition:

- 'at a distance' means that the service is provided without the parties being simultaneously present physically;

- 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

- 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request. Unsolicited services, that is, services supplied without having been individually requested, are therefore not covered.

101. Furthermore, 'information society services' under the scope of this recommendation are normally provided for remuneration. Direct or indirect payments are concerned. A service provided without direct economical or societal compensation but financed directly or indirectly by marketing comes within this definition of 'information society services'.

**2. General principles**

102. During the drafting of the recommendation it was deemed necessary to underline a number of general principles which are not aimed at establishing legal obligations. Their purpose is to clarify the interpretation and implementation of other provisions of the appendix.

103. **Principle 2.1** states that the collection and processing of personal data in connection with the use of profiling methods must uphold individuals' fundamental rights and freedoms and in particular their right to respect of privacy and prohibition of discrimination.

104. This principle asserts that over and above the strict application of Convention 108, broader care must be taken regarding the way in which profiling techniques may pose a threat to private life, understood as an individual's capacity for self-determination. For example, specifically targeted publicity profiling, even though it may be compatible with data protection legislation, could constitute an undue limitation on an individual's capacity for choice.

105. In this recommendation the principle of non-discrimination is not seen as a ban on differential treatment, since differences in the treatment of individuals as a result of profiling are acceptable provided they are justified.

106. Profiling clearly permits, and is aimed at, the differentiation of service users or citizens. For instance, it makes it possible to target advertising at individuals according to their needs, to calculate the cost of a product in line with consumer characteristics and categories or, indeed, to confine the award of benefits to persons who appear to match a given profile. Such uses of profiling can be regarded as legitimate. What is proscribed is the use of profiling techniques producing arbitrary negative effects in breach of the law, such as refusal to supply a service or product to individuals where profiling suggests that they may be foreigners or that they do not subscribe to the provider's philosophy or to persons profiled as having or likely to have a criminal record, without the criterion highlighted by the profiling being justified or relevant to the nature or characteristics of the product or service.

107. **Principle 2.2** moreover requires transparency, which is nonetheless reduced in view of the very nature of profiling. This clearly does not entail full transparency but a balanced approach to the interests at stake.

108. **Principle 2.3** contains two points. The first is already to be found in certain European Union texts and concerns the promotion of what is commonly termed "*privacy enhancing technologies or "privacy by design".* It refers in particular to the promotion of software applications enabling Internet users to object, or agree[17], if necessary in an informed and explicit way to data collection for profiling purposes, or to access and if need be correct the profile assigned to them, etc. Some software will allow greater transparency and give ways to educate users.

109. The second point is more innovative and introduces into the data protection field the same principle found in the field of the protection of intellectual property. It involves the prohibition of the development and use of any technology designed to circumvent technical data protection measures aiming at protecting the respect of private life. It is unacceptable for service providers in the information society or experts to be able, as a result of web bugs or security holes in software, to collect data even though the data subject had sought to protect himself or herself against such processing by installing new software or parametrising existing software.

## 3. Conditions for personal data collection and processing in connection with profiling

### A. Lawfulness

110. **Principles 3.1, 3.2 and 3.3** lay down basic principles, arising out of Article 5 of Convention 108, and apply them to processing using profiling methods. For example, the use of such technology must be fair and lawful, which precludes the collection of data by non-transparent means or for undisclosed purposes. This Article prohibits, for example, data collected by the use of search engines being used

[17] See Article 29 Data Protection Working Party's Opinion 2/2010 on online behavioural advertising, in particular the analysis of consent and its characteristics.

in profiling systems for advertising purposes without the person concerned being made aware of this fact or having obtained the relevant prior consent, thus reflected in Principle 3.4. The lawfulness of profiling may be challenged where such profiling pursues a discriminatory aim. Lastly, the use of profiling methods must pursue specified and legitimate aims.

111. Sub-paragraph 2 of paragraph 3 underlines the need for the data processed to be appropriate. This warrants several observations. By definition, profiling works on statistical inferences which are not immediately foreseeable. For example, if one processes chocolate consumption and finds a correlation with an interest in far-off destinations, can one subsequently say that statistically at least this is a relevant data item for someone wishing to sell exotic holidays, even though it was not relevant at the outset? The Council of Europe considers that the relevance must be assessed more broadly, but must exclude data the nature of which at the outset do not appear to have any link with the anticipated result. In other terms, if the aim is to sell a major consumer product, it is irrelevant to ask questions about the academic success of the individuals concerned, whether or not they have a goldfish or if they read Asterix. The use of such data in "data-mining" operations may indeed reveal certain correlations but these fall outside the context of the normal use of such data, conflicting with the reasonable presumptions of the individual assigned a profile on the basis of such data. This, accordingly, is unfair processing.

112. **Principle 3.3** lays down, for processing using profiling methods, the principle of a limitation to the duration of data storage. The period of use of a profile assigned to a data subject must not exceed the time required to achieve the aims for which the data were collected and processed. This rule must take into account the value to be derived from maintaining for a period of time the data gathered in respect of an individual so as to be able to modify that person's profile. For example, if a large store obtains my consent to send me advertising based on my purchasing profile, the data relating to my purchases should be kept for the whole period of my contract with the supplier. Moreover, where a contractual relationship does not exist and consent to send advertising based on data subject's purchasing profile has been duly obtained, it seems advisable to recommend that data related to purchases are kept for a limited amount of time (e.g. 12 months as stated for profiling activities in loyalty programmes in Italy).

113. **Principle 3.4** deals with the applicability of general lawfulness requirements to the profiling process. It should be noted that Principle 3.4 applies to the profiling process as such and not to the purpose for which the process is being used. For example, if profiling is used in connection with a marketing operation– above and beyond the conditions of lawfulness attached to processing for marketing purposes – Principle 3.4 adds conditions of lawfulness specific to the use of profiling in the context of that marketing processing. Accordingly, given that the state is lawfully authorised to combat fraud, there must also be provision for it to be allowed to create data-warehouses and use data-mining techniques.

114. Sub-paragraph a) specifically concerns situations in which profiling is provided for by law, in particular with regard to the identification of people at-risk, potential fraudsters or people eligible for social benefits. The term "provided for by domestic law" means that domestic law contains rules which expressly lay down provisions and safeguards required by, or exceptions to, the principles in the recommendation. To adhere to the requirement "provided for by law", any interference with fundamental rights or freedoms, and in particular the individual's privacy, must therefore have a legal basis in domestic law and be performed in accordance with domestic law[18].

115. The term 'provided for by law' could have two implications. Firstly, the law can provide for profiling by regulating the possibility – and not the obligation – of profiling. For instance, the taxation authorities are entitled to control the revenues of citizens in case of suspected fraud. It is important that taxation regulation provides the possibility of using profiling methods to detect the cases and regulate the use of these profiling techniques. It does not mean that the taxation authorities will necessarily use these possibilities.

[18], § 50, Recommendation (97) 18 concerning the protection of personal data collected and processed for statistical purposes.

116. Secondly, profiling can be necessary for compliance with a legal obligation but in that case the use of profiling techniques must be made possible by law. The legal obligation can make profiling necessary in order for the controller to be able to comply with the law. An example might be given as regards money laundering regulations. Banks are obliged to detect operations which might be considered as money laundering operations and in doing so are committed by law to using profiling mechanisms.

117. In these cases, where profiling is 'necessary for compliance with a legal obligation'; the recourse to profiling techniques is admissible only if this recourse is 'provided for by law'.

118. Subparagraph b) is specifically concerned with optional profiling. In such cases, profiling must be 'permitted' by law. The words '**permitted by law**' refer to profiling in accordance with the principles of this recommendation that is **not explicitly prohibited** by domestic law. Principle 3.4.b. also states that profiling is dependent for its legitimacy on:

- **the free, specific and informed consent of the data subject**. Consent may be used as the legal basis for profiling. Consent, as a legal basis, has not been given any distinct scope but is deliberately included among the lawfulness principles requiring fulfilment of a common prerequisite (not being expressly prohibited by law). The aim is to cover cases arising in certain states where the use of profiling is unlawful even though prior consent has been obtained.
Consent must be free, specific and informed[19]. For example, consent may be given online, for example, by clicking an 'I accept' button. In other cases, it may be implied, for example, through the provision of a hyperlink to a page explaining the profiling technique used for the processing.

**- the performance of a contract with the data subject.** In this case, profiling is used in connection with performance of a contract or implementation of pre-contractual measures. The contract could also have been concluded at the data subject's request. One example might be the profiling performed by a bank in connection with a personal loan application in order to assess a borrower's likely credit-worthiness. It should be noted that the use of profiling must be necessary for the performance of the contract or the implementation of pre-contractual measures.

- the **performance of a task carried out in the public interest** or of a statutory requirement. For example, a bank might have to profile its customers because of a statutory requirement to report suspicious money movements to government bodies responsible for combating money-laundering and to use profiling for this purpose.

- **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.** The use of profiling for detecting suspicions of fraud in the case of insurance contracts by an insurance company might be an example. The difficulties may arise from the interpretation of what "legitimate interests" means; and balancing them against data subjects' fundamental rights and freedoms. In this case, the ultimate concern should not be so much in terms of the increased risks arising out of profiling but an overall test of legitimacy, proportionality and security of processing. Thus, the use of profiling for marketing purposes is subject to a two-fold legitimacy test: firstly, 'Is the marketing purpose legitimate?' and secondly, if so, 'Is it legitimate to use profiling for this purpose?'

- **the necessity in the vital interests of the data subject**. This might include genetic profiling of members of the same family to identify a predisposition to contract certain diseases, thus allowing preventive treatment for those members of the family whose lives might be in danger. These cases however remain rare.

[19] See, Opinion 2/2010 of the Article 29 Working Party, mentioned above.

119. **Principle 3.5** prohibits in principle the profiling of persons unable to freely express their consent, especially, for example, adults with incapacity as well as children, within the meaning of the United Nations' Convention on the Rights of the Child adopted in New York on 20 November 1989. The authors consider that such a prohibition in principle is necessary in view of the dangers of manipulation and negative discrimination represented by profiling in respect of these categories of individual. The prohibition can be lifted by member states where profiling is used in the legitimate interests of the individuals concerned (for example, to obviate a particular danger of which these persons must be made aware, or to enable them to benefit from a form of assistance for which they have a specific need) or if there is an overriding general interest provided for by law and offering appropriate guarantees.

120. **Principle 3.6** stipulates that where the consent of the data subject is required, the controller must prove that he or she has fully complied with the obligation to provide information which is detailed in Chapter 4.

121. **Principle 3.7** deals with anonymous access to goods and services and invokes what is known as the personal data 'minimisation principle'. Particularly online, an individual wishing to find out about goods or services or to access them should not, in principle, have to provide any information apart from the characteristics of those goods or services. An individual should only be identified, which could ensure a transaction's security, once he or she has placed an order and for the purposes of fulfilling that order. Access to information about goods and services should therefore, as far as possible, be anonymous and non-profiled. Knowing that it is technically possible to adapt the provision of information to the user, non-profiled access to information made available online is also a precondition for users' effective exercise of the freedom of expression.

122. **Principle 3.8** prohibits the distribution and use of software designed to observe and monitor use of a terminal or communication network, which would make it possible to collect data and use profiling methods without the data subjects' knowledge unless expressly provided for by domestic law and accompanied by appropriate safeguards. For example, it is unacceptable that as a result of security holes in software available on the market, applications may install themselves on an individual's computer or simply monitor all or selected uses of a terminal or network in order to build up user profiles.

123. The proposed text does not refer to other operations regarding the processing of communications by private companies which, as is already provided for in most member states, record electronic communications where such recording is in the context of lawful business practice, in order, for example, to constitute proof of whether or not a commercial transaction has taken place.

124. In today's technological climate, users of the Internet and communications networks in general are tracked and profiled using opaque technology such as web bugs and cookies. As we have seen above, profiling performed using a communications terminal raises a serious problem of legitimacy, since the user is thus profiled in spheres of privacy that should in principle be separate but which he or she accesses through that terminal. At present, multinational firms manage to capture a large part of each Internet user's click stream on individual databases and are thus able to build 'comprehensive' personal profiles, that is, affecting multiple areas of an individual's life. Technically, this type of profiling by the terminal can be regulated only if network operators and manufacturers of communications terminals take technical steps to prevent the monitoring of user behaviour and the transmission of the resulting profiles to unauthorised third parties. This principle does not prevent online profiling but encourages the information and communications industry to produce terminals that are as transparent as possible. This principle reflects Principle 2.3 above.

**B. Data quality**

125. **Principles 3.9 and 3.10** require the controller to take all possible steps to ensure high-quality profiling. This means, for example, that he or she must use both anonymous and personal data that are accurate and up-to-date and also that the inference rules used in data-mining should have the lowest possible positive and negative error rates. Thus it would not be lawful for a bank to use a profiling system for defaulters based on inaccurate or out-of-date data, since in this case the profiles ultimately attributed to identified individuals would in all likelihood be subject to a substantial margin of error. The algorithms employed during the data-mining stage must be selected and used in accordance with best practice in this field. Last but not least, the controller using such systems must periodically re-evaluate the pertinence of the profiles generated. For example, it may be that chocolate consumption is no longer regarded as a factor which can statistically be correlated with a predilection for long-haul journeys.

126. It should be noted that data accuracy is a concomitant data protection requirement. This provision does not require the establishment of supervisory arrangements to check the accuracy of data. What is necessary is to correct inaccuracies while recognising that the three stages of profiling, including the application of an established correlation to identified or identifiable individuals, are a continuous process. This requirement needs to be interpreted in a reasonable manner, having regard to the purpose of the data processing, since the impact of inaccuracies on identified or identifiable individuals would clearly differ according to whether they concern, for example, the insurance or the direct marketing sectors.

**C. Sensitive data**

127. **Principle 3.11** stipulates that sensitive data may only be processed for profiling purposes if there are appropriate domestic legal safeguards. This principle is based on Article 6 of Convention 108 which provides, though this is not an exhaustive list, that personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life and criminal convictions, may not be processed automatically unless domestic law provides appropriate safeguards.

128. It is for member states' domestic legislation to determine what constitute legitimate exceptions regarding the use of sensitive data for profiling purposes. For example, the domestic law of all the member states of the European Union that have applied Directive 95/46/EC has to include the exceptions listed in Article 8 of that directive.

129. These appropriate and legitimate guarantees may include the data subject’s consent or the statutory regulation of the intended profiling process in order to maintain the confidentiality of the data processed or produced by profiling and to ensure that use of profiles is strictly confined to types of processing that are legitimate. Moreover, the principle specifically requires explicit consent in the event of profiling using sensitive data in cases where consent is required.

**4. Information**

130. **Principle 4.1** sets out the nature of the information to be given to the data subject by the controller and concerns two particular sets of circumstances: situations where the data collected are to be used for immediate profiling and ones where the profiling occurs after the collection process, but always when the original purpose was to use profiling**.** The use of profiling cannot be concealed from the data subject, and the controller must use all reasonable means (website information, etc.) to inform data subjects of the existence of the profiling and of their rights. Such information must be provided rapidly and full use must be made of the potential of information and communication technologies. In particular, when profiling takes place on line, such technologies make it possible to inform the individual concerned immediately.

131. However, it is necessary to specify that the manner and extent of such provision of information must be appropriate and adapted to the circumstances. It was therefore felt that various forms and means of communication could be used as required according to the nature or scale of the profiling. It was also acknowledged that information on the use of profiling might, by its very nature, be a disproportionate burden on the controller, having regard to all its possible forms and circumstances and the limits imposed by the means of communication used The terminology used and the amount of detail in the information should, however, be such as to allow the data subject to grasp easily, but only in general terms, the purposes and significance of the profiling. Furthermore, the controller is not required to provide the information if the profiling process is regulated by domestic law.

132. A distinction should be drawn between the obligation to provide information about the purposes for which the profiling is carried out (4.1.b) and the envisaged effects of the attribution of the profile to the data subject (4.1.f, last sub-paragraph). For example, the purpose of credit scoring is to assess the data subject's creditworthiness, whereas the envisaged effect of the profiling will be the granting or withholding of credit, the granting of credit on more costly terms, and so on. The envisaged effects of attributing a profile are not always foreseeable when data collection takes place or when the profile is applied. It is for this reason that this safeguard has been included under principle 4.1.f, which relates to safeguards left to the member states' discretion. These safeguards should moreover be applied in an appropriate manner in the light of the specific circumstances.

133. **Principles 4.2 and 4.3** distinguish between two situations when an individual is required to receive the information specified in Principle 4.1, namely whether or not the data are collected directly from that individual. Principle 4.3 is based directly on Article 11 of Directive 95/46 EC.

134. **Principle 4.4** constitutes an additional safeguard in relation to Principle 4.1. As already mentioned, profiling is a technical process permitting the attainment of a given goal. Data recorded without the initial intent of applying profiling could subsequently be used for that purpose. In such cases the data controller should also be obliged to provide the data subject with the information listed in Principle 4.1, in particular when the profile is applied. If a data controller decides to use data for a purpose other than that for which they were initially collected, this should be regarded as a new collection operation and the obligation to provide information as set out in Principle 4.1 should apply.

135. **Principle 4.5** stipulates the circumstances where the obligations under principles 4.2 and 4.3 do not apply.

136. **Principle 4.6** establishes a common-sense principle. The way in which the data subject is informed of the use of profiling methods shall vary according to the context of the use of such methods. For example, a pop-up may warn an Internet user that the banner advertisements he or she receives are the result of profiling. If, however, the data subject is to receive a visit from tax inspectors as a consequence of the profiling of taxpayers, it is unlikely that he or she will be informed in the same way.

**5. Rights of data subjects**

137. **Principle 5.1** states that the data subject is entitled to know about the personal data concerning him or her and the logic which have served as a basis for the profiling. It is indeed essential that a data subject exercising the right of access should be informed of the statistical method and inferences used for his or her profiling, the logic underpinning the processing and the envisaged consequences of the profile's attribution.

138. In addition, if the profiling involves new risks, specific safeguards should be established in order to compensate for it. Principle 5.1.c allows states which so wish to offer a stricter guarantee while retaining the possibility of issuing a reservation.

139. Without an understanding of these elements there could be no effective exercise of other safeguards - the right to object and the right to complain to a competent authority.

140. For example, individuals receiving quotes for insurance against water damage must be informed of the logic followed to calculate the prices quoted. Was their risk profile based on statistics? Which of their personal circumstances were taken into account in calculating the insurance premium? Data subjects will be in a position to state their grounds for objecting only if they are in possession of these elements.

141. Information on the logic underpinning the processing should not be confined to cases involving automated decision-making, as that is not the sole goal of profiling. States may extend this obligation to a number of cases, but without requiring a disproportionate effort on the controller's part and without breaching the rights and freedoms of others, in particular trade secrets.[20] The data subject is in principle not entitled to receive the anonymous data used for profiling. Moreover, the data controller is only required to provide sufficient information to allow an understanding of the possible consequences of the profile's attribution.

.

142. **Principle 5.2** draws on Article 8c of Convention 108 and enables data subjects to obtain the correction, deletion or blocking of their personal data, as the case may be

143. **Principle 5.3** grants the data subject, subject to exceptions, the right to object to the use of his or her data in the context of profiling for marketing purposes. For example, if an individual is given to understand that the advertising he or she receives online or that the suggested choice of sites he or she might wish to consult are tailored to his or her profile, he or she should be able to object without giving any particular reasons. The right to object to profiling when it is carried out for other than marketing purposes requires the data subject to provide compelling legitimate grounds. For example, individuals refused a loan because of the location of their home, the fact that they do not have a telephone contract and that they are not in stable employment, which statistically speaking are indications that they would be unable to repay, could object to the use of such a profile by showing that the change of employment was due to the successive bankruptcies of their previous employers, forcing them to move house in haste because of a new job and that this explained the fact that they did not have a telephone contract.

144. **Principle 5.4** nevertheless provides for additional safeguards against the arbitrary use of the limitations to the rights established in this chapter.

145. It should be noted that some rights, such as the individuals' right of access to information relating to data about him or herself, may be restricted if the reasons enshrined in Chapter 6 are real (national safety, public safety, etc.). See for example Article 6 of Recommendation R (87) 15 regulating the use of personal data in the police sector and Article 17 of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

146. In this case a reasoned decision refusing or restricting rights should be notified to the data subject by any means allowing a record of the notification to be kept. However, it is possible not to give reasons where this might jeopardise the very purpose served by a restriction.

147. This principle has been established to take account of the difficulty of performing certain functions incumbent on a state, in particular in the field of policing and keeping law and order. A balanced approach should allow the effective performance of these functions without depriving individuals of their rights. For example, the rights in question may be restricted only for as long as the grounds for the restriction exists. It has to be established that the reasons for limiting access to data are provided

[20] See considering 17 of the recommendation.

for in law and are necessary in a democratic society. In democratic societies, such a necessary decision implies a 'pressing social need' and has to be proportional to the legitimate aim pursued. It is important to ensure that the reasons put forward for refusing or limiting access are not used to get round the safeguards established to protect the individuals concerned. Lastly, if individuals are given no reason for a refusal or restriction they must be informed of the possible means of challenging such decisions.

148. **Principle 5.5** refers to cases where the use of profiling alone may lead to a decision having legal effects on the data subject (for example, is the person in question, in view of his or her profile, entitled to a particular social benefit?) or having a significant effect on him or her (for example, such a person, in view of his or her profile, is not deemed suitable for a loan of X amount of Euros). This principle gives the data subject the right to object to the decision. There are exceptions to this principle wherever the law provides for use of such methods or where the decision has been taken in the context of a contract or pre-contractual measures (subject to compliance with the principles relating to the lawfulness of profiling, data quality and the right to information), the use of profiling for recruitment decisions is possible provided there are appropriate guarantees enabling the data subject to put forward his or her point of view, in particular in the course of an interview during which he or she may have the opportunity to substantiate the inaccuracy of the data in the profile, the irrelevance of the profile to his or her particular situation, or other arguments.

**6. Exceptions and restrictions**

149. **Principle 6.1** is drawn directly from Article 9 of Convention 108 (itself being drawn from the second parts of Articles 6, 8, 10 and 11 of the ECHR) and determines the authorised exceptions to the principles established in Chapters 3, 4 and 5. The case law of the Court contains detailed considerations on the grounds for restrictions, in particular with regard to the concept of a necessary measure, which may vary according to circumstances. By allowing for exceptions, the recommendation takes a balanced approach, leaving states a margin of discretion in duly justified circumstances

150. Chapter 2 is not mentioned under Principle 6.1 since, as stated above, it does not seek to establish legal obligations which may be subject to derogations.

**7. Remedies**

151. **Principle 7.1** requires there to be appropriate remedies for the data subject in the event of a breach of the regulatory provisions giving effect to the principles laid down in the recommendation. Such remedies presuppose the intervention of an independent authority, whether a court or independent body as understood by the additional protocol to Convention 108, i.e. having powers of investigation and able to order appropriate sanctions.

**8. Data security**

152. **Principle 8.1** deals with the technical and organisational steps which must be taken to ensure data security. One way of implementing this recommendation is by legal means. Other means might be considered involving the establishment of internal policies and procedures since it is not enough to provide full protection of personal data by laying down legal rules; practical precautions also have to be taken by the controller to avoid any accidental or malicious processing incidents.

153. **Principle 8.2** stipulates that the controller is responsible for taking the technical and organisational steps referred to above.

154. **Principle 8.3** provides for the additional safeguard that controllers who use profiling techniques comprising particular risks for data subjects, in connection with various criteria (type of data

processed, impact of the decision taken or the effects of the profiling, nature of the collection network, etc.) must, where necessary, appoint within their organisation a person whose status guarantees his or her independence and who is responsible for ensuring compliance with the principles of Convention 108 and this recommendation, and that this personal data protection official is able to offer advice on the profiling methods used by the controller.

155. The appointment of such a person need not prevent data controllers from appointing data processing and personal freedom correspondents, possibly with more extensive powers and responsibilities

156. **Principle 8.4** provides that if profiling operations are contracted out to a third party the controller must make provision for adequate safeguards to ensure that this processor actually complies with the requirements concerning lawfulness and security detailed in the appendix to this recommendation. [21]

157. **Principle 8.5** provides for an additional safeguard against possible overuse when the statistical results are used for profiling purposes. This requirement is based on Recommendation No R (97) 18 which lays down conditions for lawfulness in relation to the collection and processing of personal data for statistical purposes and in particular its Principle 3.3 which requires the personal data to be anonymous as soon as it is no longer of necessity to have it in identifiable form.

## 9. Supervisory authorities

158. **Principle 9.1** provides that member states shall mandate one or more independent supervisory authority to monitor compliance with domestic legislation implementing the principles set out in this recommendation. These independent authorities as well as the extent of their powers of investigation and intervention are covered by the provisions of the Additional Protocol to Convention 108. [22]

159. **Principle 9.2** provides a possibility of introducing a notification requirement or a prior checking mechanism by of the independent supervisory authority referred to in Principle 9.1. It should be underlined that this principle does not aim to impose on member states a legal obligation to set this up but to foresee such a possibility wherever the processing of personal data using profiling appears to entail specific and special risks for the protection of privacy. In cases where the controller has provided for appropriate measures, such as advice from a data protection official, it is open to member states to exempt that controller from this requirement for notification or prior authorisation.

160. Lastly, **Principle 9.3** requires that the authorities inform the public, in their annual reports for example, of the content of the recommendation and educate them on the risks associated with profiling.

[21] See also, Opinion 1/2010 on the concepts of "controller" and "processor" by Article 29 Working Party, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2010_en.htm

[22] See explanatory report on Article 1§2a of the Additional Protocol to Convention No. 108.