



Strasbourg, 5 March 2009

T-PD-BUR (2009) 02 rev

**BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION
FOR THE PROTECTION OF INDIVIDUALS
WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA**

(T-PD-BUR)

9-10 February 2009
17th meeting, Strasbourg
Building "Agora", Room 2

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

As resulting from the 17th Bureau meeting (February 2009)

Brackets [...] indicate text that the Bureau thinks of deleting or moving

Secretariat document prepared by
the Directorate General of Human Rights and Legal Affairs

1. Considering that the aim of the Council of Europe is to achieve ever closer union among its members;
2. Noting that information and communication technologies allow the collection on a large scale of anonymous or personal data. Noting that these technologies are often convergent, with hitherto unknown capacities for the capture, communication and processing of information [relating to the interactions of individuals with their environment, whether physical or digital];
3. Noting that this collection may use in particular the processing of traffic data and user queries on the Internet, the recording of consumer buying habits and activity, the processing of geo-location data concerning mobile telephone users, the data collected by video surveillance cameras and by RFID systems, foreshadowing the "internet of things", and finally by biometric systems;
4. Noting that data thus collected are processed by calculation, comparison and statistical correlation softwares, with the aim of producing profiles. Noting that profiles result in the main from matching data of several individuals. Noting that these operations may be done at a low cost;
5. Noting that profiling consists in attributing a profile to an identified or identifiable individual for the purpose of predicting personal preferences, behaviour and attitudes and for taking decisions about him/her;
6. Considering that profiling may result in attributing to an identified or identifiable individual characteristics of a group to which he/she has been associated, but which are not necessarily his/hers. Considering that, in this respect, the result of profiling is not exclusively based on personal data that the data subject has communicated to the data controller or of which he/she can reasonably presume the controller has knowledge;
7. Considering that profiles, when they are attributed to a data subject, constitute new personal data;
8. Considering that resorting to profiling may, for the person who uses it as well as the person to whom it is applied, correspond to legitimate interests, such as a better market segmentation, the analysis of risks, frauds, the adaptation of offer to demand, [and that both may gain advantages from it, for instance in the economical and social spheres];
9. Considering however that attributing a profile to an individual may result in depriving him/her from accessing to certain goods or services, such as bank credit, insurance, online media services, or affect their price;
10. [Considering furthermore that profiling techniques, when they highlight 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 108, hereafter "the Convention") and other data, can enable the deduction of sensitive data concerning an identified or identifiable person, on the basis of his/her non sensitive personal data;]
11. [Realising that, in cases where profiling is based on systematic observation by a third party of the use made of a telecommunications network or terminal, there is a major risk of matching data collected and processed in operations carried out by different file controllers and using them for mutually incompatible purposes;]

12. Considering that the use of profiles without precautions and specific safeguards could severely damage human dignity, as well as fundamental rights and freedoms, including economic and social rights;
13. Convinced that it is therefore desirable to regulate profiling as regards the protection of personal data in order to safeguard the fundamental rights and freedoms of individuals, in particular the right to privacy;
14. Recalling in this regard the general principles on data protection in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg 1981, European Treaty Series No. 108);
15. Taking into account 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;
16. Considering that the protection of human dignity and fundamental freedoms in the framework of profiling can be effective if and only if all the stakeholders contribute together to a fair and legitimate profiling of individuals.

Recommends that the governments of member states:

1. take measures to ensure that the principles set out in the Appendix to this recommendation are reflected in their legislation and practice;
2. arrange for broad dissemination of the principles set out in the Appendix to this recommendation among individuals, public authorities and bodies which participate in and use profiling in both the public and the private sectors, in particular in the field of information society services, such as designers and deployers of software for electronic communications terminal equipment, profiles designers, internet access providers and information society services providers, as well as among the bodies responsible for data protection and the standardisation bodies;
3. encourage such individuals, public authorities and bodies to introduce ethical codes and technologies based on the Appendix to this recommendation.

Appendix to the recommendation

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 and manpower. Where the individual is not identifiable the data is deemed "anonymous".
- b. "Sensitive data" means personal data revealing the racial origin, political opinions and religious or other convictions, as well as personal data on health, sex life or criminal convictions, as well as other data defined as sensitive by domestic legislation.
- 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. "Profiling" means an automatic processing of data whose aim is to apply to an individual an evaluation, classification or decision on the basis of matching of data relating to individuals.
- e. ["Profile" refers to a set of data characterizing a category of persons and that is intended to be applied to a specific person.]
- f. "Information society service" refers to any service at a distance, by electronic means and at the individual request of a recipient of services.

2. Scope

- 2.1 This recommendation applies to the collection and processing of personal data which contribute to and resort to profiling.

3. General principles

- 3.1 Respect for fundamental rights and freedoms, notably the right to privacy, must be guaranteed during the collection and processing of personal data subject to this recommendation.
- 3.2 Collection and processing must not lead to discriminatory measures contrary to human dignity.
- 3.3 [In the case that an individual is subject to a decision taken on the sole basis of profiling, he/she should be allowed:
 - to oppose this decision or
 - to benefit from appropriate safeguards such as the right to access information specified at article 6 and to put forward his/her viewpoint.]

4. General conditions for data collection and processing for the purposes of profiling

A. Lawfulness and fairness

4.1 Profiling individuals shall be fair, lawful, proportionate and for legitimate purposes.

4.2 Moreover, profiling in the framework of processing of personal data may be performed/is allowed only:

- a. if it is explicitly provided for by law
- b. or, failing that, if the law does not forbid it, under the following conditions:
 - the data subject or his or her legal representative has given his or her free, specific and informed consent or
 - it is necessary for the purposes of the legitimate interests of the controller, except where such interests are overridden by the fundamental rights and freedoms of the data subjects.

4.3 [In order to ensure a free, specific and informed consent to the profiling, providers of information society services must ensure, if possible/by default, anonymous and non-profiled access to their services. Moreover, users of an information society service cannot be profiled without their knowledge or against their will.]

4.4 [The distribution of software allowing or facilitating the observation by third persons without the data subjects knowing of the use being made of a given terminal or telecommunications network should be prohibited.]

4.5 [Providers of access to telecommunications networks open to the public shall supply their customers with, or place at their disposal, appropriate generic communication software which does not permit the matching of users' behaviour without their free, specific and informed consent.]

4.6 [Personal data collected and processed exclusively for statistical purposes within the meaning of Recommendation No. R (97) 18 must not be used further in the framework of profiling.]

B. Proportionality and purpose

4.7 As a general rule, everyone should have access to goods or services without having to communicate personal data to the good or service provider.

C. Data quality

4.8 Appropriate measures should be taken to correct data inaccuracy factors and risks of errors inherent in profiling, so that individuals are not subjected to processing unsuited to their personal situations.

4.9 The data controller shall reevaluate periodically the quality of the data and of the statistical inferences used.

D. Sensitive data

4.10 Unless it is necessary for the pursuit of an important public interest as set out by the law, and provided that domestic law provides the appropriate safeguards, the processing of sensitive data in the framework of profiling should be prohibited.

5. Information

5.1 When personal data is collected, the data controller must inform in advance the data subjects of the fact that their data may be used to feed profile creation systems.

5.2 When a personal data processing applies a profiling system to a data subject, he/she must receive in advance the following minimum information:

- a) the existence of profiling,
- b) the purposes of the profiling made,
- c) the categories of data used;
- d) the identity of the controller of the file and if necessary his/her representative;
- e) the existence of appropriate safeguards;
- f) where the profiling is geared to, or has the effect of, altering the prices for goods or services for the data subject, the data controller must inform him/her explicitly, specifically and in advance of the profiling procedure.

6. Rights of data subjects

6.1 The individual who is being profiled is entitled to obtain, at his/her request, from the data controller communication of:

- a) personal data about him/her,
- b) the logic underpinning the processing of data about him/her and that was used,
- c) the significance and consequences of the profile attributed to him/her,
- d) the reliability of the profiling operations, specifying the statistical rate of false negatives and false positives.

7. Supervisory authorities

7.1 The member states shall mandate one or more independent authorities to monitor compliance with the domestic legislation implementing the principles set out in this recommendation and having in this respect the necessary powers of investigation and intervention.

7.2 In the case of processings that use profiling and entail special risks with regard to the protection of privacy and personal data, member states may foresee:

- either that controllers have to notify processings in advance to the supervisory authority,
- or that these processings are subject to prior checkings by the supervisory authority.