



Strasbourg, 2 October 2009

T-PD-BUR (2009) 02 rev 4

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

(T-PD)

2-4 September 2009
25th plenary meeting, Strasbourg
Building "Agora", Room 1

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

As resulting from the 25th plenary meeting

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 (ICTs) allow the collection and processing on a large scale of data, including personal data, in both the private and public sectors, noting that continuous development of convergent technologies poses new challenges as regards collection and further processing of data;
3. Noting that this collection may concern traffic data and user queries [in search engines] on the Internet, consumer buying habits and activity, geo-location data concerning telecommunication devices users, as well as the data stemming in particular from video surveillance cameras, biometric systems and by RFID systems, foreshadowing the "internet of things";
4. Noting that data thus collected are processed namely by calculation, comparison and statistical correlation softwares, with the aim of producing profiles that could be used in many ways by matching data of several individuals. Noting that these operations may be done at a low investment;
5. Noting that profiling is an automatic data processing technique whose aim is to apply a set of data characterising a category of persons ("profile") to an individual for the purpose of predicting personal preferences, behaviours and attitudes;
6. Considering that, through this linking of a large number of individual although anonymised observations, the profiling technique is capable of having an impact on the persons concerned by placing them in predetermined categories or groups;
7. Considering that profiles, when they are attributed to a data subject, generate new personal data which are not those which the data subject has communicated to the data processing controller or which he/she can reasonably presume to be known to the controller;
8. Considering that the lack of clarity (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;
9. Considering in particular that the protection of privacy and fundamental rights entails the existence of different and independent spheres of life where each individual can express and control a part of his/her identity;
10. 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, allowing the analysis of risks and fraud, and adapting offers to meet demand; and considering that profiling may thus provide benefits for users, the economy, and society at large, through enhancing the user's experience when surfing the web and delivering more relevant information and services, and that many services, content, and applications on the Internet are largely financed through online advertising;

11. Considering however that profiling an individual may result in depriving him/her from accessing certain goods or services, such as bank credit, insurance, online media services;
12. 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 deduction of sensitive data concerning an identified or identifiable person or "groups" of people with the same characteristics. Considering that such profiling can expose individuals to particularly high risks of discrimination and attacks to their personal rights and dignity;
13. Considering that the use of profiles, that has to be in any case legitimate, without precautions and specific safeguards could severely damage human dignity, as well as 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 of individuals, in particular the right to privacy;
15. Recalling in this regard the general principles on data protection in Convention 108;
16. Recalling the necessity to comply with the already existing principles as set out by other relevant Recommendations of the Council of Europe, in particular Recommendation Rec (2002) 9 on the protection of personal data collected and processed for insurance purposes and Recommendation Rec No. R (97)18 on the protection of personal data collected and processed for statistical purposes;
17. 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;
18. 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 lawful profiling of individuals;
19. Taking into account that the mobility of individuals, the globalisation of markets, and the use of new technologies necessitate transborder exchanges of information also in the framework of profiling and require equivalent data protection in all the member states of the Council of Europe;

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 and bodies which participate in and use profiling 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 service providers, as well as among the bodies responsible for data protection and the standardisation bodies;
3. encourage such individuals, public authorities and bodies to promote self-regulation mechanisms such as codes of conduct ensuring respect for privacy and data protection, as well as develop 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 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 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. "Profile" refers to a set of automatically generated 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 for the purpose of 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 legal 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 a natural or legal person, public authority, agency or any other body which process personal data on behalf of the controller.

2. Scope

- 2.1 This Recommendation applies to the collection and processing of personal data using profiling in the private sector.
- 2.2 Member states may extend the application of this Recommendation to the public sector.

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 Profiling must not lead to discriminatory measures of any kind.
- 3.3 Member states shall encourage the development and the use of privacy enhancing technologies, in particular communication software which does not permit the profiling of users without their free, specific and informed consent.

4. Conditions for personal data collection and processing using profiling

A. Lawfulness

- 4.1 The profiling of individuals shall be fair, lawful, proportionate and for specified and legitimate purposes.
- 4.2 Personal data used in the framework of profiling shall be adequate, relevant and not excessive in relation to the purposes for which they are collected or are to be processed further.
- 4.3 Personal data used in the framework of profiling shall 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 obtained and processed.
- 4.4 Moreover, processing of personal data in the framework 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; consent must be explicit where the processing concerns sensitive data, or
 - profiling 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
 - profiling 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 except where such interests are overridden by the fundamental rights and freedoms of the data subjects, or
 - if it is necessary for the vital interest of the data subject.
- 4.5 As much as possible, and unless the service required necessitates knowledge of the data subject's identity, everyone must have access to goods or services without having to communicate personal data to the good or service provider. In order to ensure a free, specific and informed consent to the profiling, providers of information society services must ensure, by default, anonymous and non-profiled access to their services.
- 4.6 The distribution and use of software aiming at the observation or the monitoring in the framework of profiling without the data subject's knowledge of the use being made namely of a given terminal or electronic telecommunications network is unlawful unless expressly provided for by domestic law and unless appropriate safeguards are provided.
- 4.7 The controller shall not use for profiling the data legitimately gathered and processed for other purposes, unless appropriate safeguards are provided.
- 4.8 The transfer of personal data used in the framework of profiling to third parties is allowed only under the conditions set forth in Principle 4.4.

B. Data quality

- 4.9 Appropriate measures shall be taken by the controller to correct personal data inaccuracy factors and limit the risks of errors inherent in profiling.
- 4.10 The controller shall periodically and without unreasonable delay re-evaluate the quality of the personal data and of the statistical inferences used.

C. Sensitive data

- 4.11 The processing of sensitive data in the framework 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.

5. Information

- 5.1 When personal data is collected in the framework of profiling or at the time of applying the profile to the data subject, the controller must give to the data subjects explicitly and specifically the following minimum information:
- a. the existence of profiling;
 - b. the purposes for which the profiling is made;
 - c. the effects of applying the profile to the data subject;
 - d. the categories of personal data used;
 - e. the identity of the controller and if necessary his/her representative;
 - f. the duration of storage;
 - g. the existence of adequate safeguards;
 - h. 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;
 - 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.
- 5.2 Where the personal data are collected from the data subject, the controller shall give the data subject the information listed in Principle 5.1 at the latest at the time of collection, except where the data subject has already been informed.
- 5.3 Where personal data are not collected from data subjects, the controller shall give the data subjects the information listed in Principle 5.1 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.

The obligation to inform the data subjects does 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 must be provided for.

- 5.4 Information provided to the data subject shall be appropriate and adapted to the circumstances.
- 5.5 It shall be incumbent on the controller to prove that the user agreed to profiling after receiving adequate information.

6. Rights of data subjects

- 6.1 The rights of data subjects to obtain the personal data concerning them, knowledge of the profile, or correction, deletion or blocking, shall not be limited unless such limitation constitutes a measure prescribed by law and necessary in a democratic society for protecting state security or public safety, the monetary interests in the state, preventing or punishing criminal offences, or protecting the rights and freedoms of others.
- 6.2 In that case, the rights may only be limited for as long as the ground of limitation persists.
- 6.3 The grounds for limiting the rights of data subjects shall be stated in writing. Where their rights are limited, they should be informed of the right to lodge with the competent authority a request for verification of the lawfulness of processing.
- 6.4 Unless the law requires profiling in the framework of personal data processing, the data subject shall 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 shall no longer involve the use of the personal data of the data subject.
- 6.5 Where a person is subject to a decision having legal or other significant effects on him or her, taken on the sole basis of profiling, he or she must be able to object to the decision unless the law permits it and sets out the measures for safeguarding the legitimate interests of data subjects, particularly by allowing them to put forward their viewpoint. Same guarantees shall be provided if that decision was taken in the course of 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.
- 6.6 [Principles 6.1 and 6.2 also apply to the individual profile].

- 6.7 The individual who is being profiled is entitled to obtain, at his/her request and without undue delay and in understandable form, from the data controller communication of:
- a. personal data about him/her;
 - b. the logic underpinning the processing of personal data about him/her and that was used to establish his/her profile;
 - c. the significance and consequences of the profile attributed to him/her;
 - d. the reliability and accuracy of the profiling operations;
 - e. the purpose of profiling made and the recipients.
- 6.8 Data subjects must be able 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.

7. Remedies

- 7.1 Domestic law shall 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 without unreasonable delay.

- 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 must 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 aggregated statistical results used in profiling may result in re-identification of the data subjects by those results.

9. Supervisory authorities

- 9.1 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.
- 9.2 Furthermore, 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 checking by the supervisory authorityand that the processings undergo retrospective checking by the supervisory authority.
- 9.3 These authorities should inform the public of the application of the legislation implementing the principles set out in this recommendation.