Strasbourg, 7 November 2019

T-PD(2019)07BISrev

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

## CONVENTION 108

# Profiling and Convention 108+: Suggestions for an update

DG I - Human Rights and Rule of Law

**Introductory note:**

The authors of the report (Profiling and Convention 108+: Report on developments after the adoption of Recommendation (2010)13 on profiling), on the basis of the structure of Recommendation (2010)13 on profiling (adopted by the Committee of Ministers on 23 November 2010), propose in the present document the amendments and additions they consider necessary to maintain the relevance of the 2010 Recommendation in the light of technological developments, uses made of such technologies and new reference standards.

## 1. Definitions

1.1. For the purposes [of the present Recommendation]:

a. The term «personal data» means any information relating to an identified or identifiable natural person (« data subject»). An individual is not considered "identifiable" if identification requires unreasonable time or effort in relation to the means at the disposal of the controller.
b. The expression «categories of data processed» means the different types of personal or non-personal data used during the profiling processing, regardless of their source and nature.
c. The expression « sensitive data » means personal data listed in Article 6 of Convention 108+.
d. The terms « processing », « controller » and « processor » refer to the definitions given by Convention 108+ in its Article 2.
e. The term « profiling » refers to « *any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements* »
f. The term « profile » refers to *« a set of data characterising a category of individuals that is intended to be applied to an individual.* »
g. The term « model » is a mathematical abstraction used in automatic learning methods, which provides a simplified description of the data to solve the task to be performed.
h. Artificial intelligence (AI) refers to any « *A set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being. Current developments aim, for instance, to be able to entrust a machine with complex tasks previously delegated to a human.* »
i. The expression « machine learning processing » means processing using particular methods of artificial intelligence based on statistical approaches to give computers the ability to "learn" from data, i.e. to improve their performance in solving tasks without being explicitly programmed for each of them.
j. The expression « Deep learning » means a set of automatic learning methods that attempt to model with a high level of data abstraction through articulated architectures of different non-linear transformations.

k. The expression « big data » identifies extremely large and heterogeneous data sets that may be analysed computationally to extract statistical inferences about data patterns, trends and correlations.
l. The expression « online intermediary services » means information society services that enable users to offer information (online research services), goods or services or to establish relations (social network access service).
m. The expression « high-risk profiling processing » refers to:
    i. profiling processing operations which operations entail legal effects or have a significant impact on the data subject or on the group of persons identified by the profiling processing;
    ii. profiling processing operations which, because of the target public and the context, involve a risk of manipulation of the data subjects;
    iii. profiling processing operations involving data qualified as special categories of data or having for purpose to detect or predict them;
    iv. profiling processing operations performed by largely established online information services on the basis of the use made of their services.

## 2. General principles

2.1. The respect for fundamental rights and freedoms, notably the right to privacy and the principle of non-discrimination, but also the imperatives of social justice, cultural diversity and democracy, shall be guaranteed during the collection and processing of personal data subject to this recommendation. Profiling processing must contribute both to the well-being of individuals and to the development of an inclusive, democratic and sustainable society.

2.2. Member states should encourage the design and implementation of procedures and systems in accordance with privacy and data protection, already at their planning stage (privacy by design), notably through the use of privacy-enhancing technologies. They should also take appropriate measures against the development and use of technologies which are aimed, wholly or partly, at the illicit circumvention of technological measures protecting privacy.

2.3. According to the 4th recital of the Preamble of Convention 108+: "Recalling that the right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms,...", profiling processing must not result in discrimination against individuals, groups or communities. They may neither undermine the dignity of persons, nor democracy.

2.4. Profiling processing must not be carried out for the purpose of manipulating vulnerable data subjects.

2.5. The use of automated decision-making systems should preserve the autonomy of human intervention in the decision-making process.

2.6. As far as possible, service providers and, in particular intermediary services should give data subjects the possibility to opt for or against profiling, or even the choice between different degrees of profiling depending on the purpose of the processing operations proposed.

2.7. Member States should ensure that the regulation of profiling processing operations is kept proportionate to the purposes they pursue, to the nature and gravity of the risks incurred by the data subjects, the targeted groups or the general interest.

2.8. Profiling processing involves different actors whose quality and role must be analysed in order to determine their responsibilities.

2.9. The use of artificial intelligence technologies known as 'deep learning' for profiling purposes poses an additional risk due to possible errors, bias and the difficulty of making the justifications for decisions taken or proposed transparent, and consequently to the full exercise of the rights of the data subjects. Their design, development and implementation require special and continuous attention with regard to the risks created and their assessment by multidisciplinary, independent teams.

## 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.

This provision is worth to be commented since, in machine learning systems, it is difficult to know *a priori* which data will allow significant correlations and, moreover, it is important to limit the profiling processing to categories of data that the data subject can reasonably expect to be taken into account in view of the legitimate purposes of profiling (example: profiling for housing access priorities that would take into account the consumption of soap operas on an online film platform).

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. Except what may be stated below, collection and processing of personal data in the context of profiling may only be performed:

a. if it is provided for by law; or
b. if permitted by law and:
   - the data subject or her or his legal representative has given her or his free, specific and informed consent;
   - is necessary for the performance of a contract to which the data subject is a party or for the implementation of pre-contractual measures taken at the request of the data subject;
   - is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the personal data are disclosed;
   - is necessary for the purposes of the legitimate interests of the controller or the third party or parties to whom the profiles or data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subjects;
   - is necessary in the vital interests of the data subject.

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

3.6. In order to be free, consent implies for the data subject the possibility of an informed choice. As far as possible, service providers and platforms should offer different services that are more or less profiled or even non-profiled depending on the service offered, in order to guarantee to the data subject a choice as regards the intensity of profiling. Consent to the profiling processing cannot be required as a condition for the performance of a service. Where consent is required, it is incumbent on the controller to prove that the data subject has agreed to the profiling processing beyond what was necessary for the performance of the service, on an informed basis, as set out in Section 4.

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

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

### B. Quality of data and algorithms

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

3.10. The controller(s) and, where applicable the processors, should periodically and within a reasonable time re-evaluate the quality of the data and of the statistical inferences used.

3.11. When acquiring data or algorithms from a third party, the controller(s) shall obtain from the third party the documentation necessary to check the quality of the data and of the algorithms and their suitability to the purpose of the processing.

3.12. Where the profiling processing is a high-risk processing operation, the controller(s) should make the control and corrective measures taken available to the supervisory authority.

### C. Special categories of data

3.13. 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.

3.14. Processing for the purpose of detecting or predicting political affiliation, philosophical, trade union or religious opinions should likewise be subject to appropriate safeguards.

## 4. Information

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

a. that their data will be used in the context of profiling;
b. the purposes for which the profiling is carried out;
c. the categories of personal data used;

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

4.2. When personal data are collected in the context of profiling, the controller should indicate the existence of a profiling activity with an icon. This icon should make it possible for anyone to automatically obtain the information listed in Principle 4.1 by linking to the website of the controller.

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

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

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

4.6. The provisions under Principles 4.3, 4.4 and 4.5 to inform the data subject 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.

4.7. The information provided to the data subject should be appropriate and adapted to the circumstances.

## 5. Rights of data subjects

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

a. her or his personal data and the categories of pseudonymised or anonymised data used in the processing operation;
b. the logic underpinning the processing of her or his personal data and that was used to attribute a profile to her or him, at least in the case of an automated decision and, in the case of the use of processing based on machine learning, which governs the functioning of the algorithm. In this case, the information must be such as to enable the data subject to understand the justification for the decisions or proposals for decisions regarding him/her;
c. the purposes for which the profiling was carried out;
d. the categories of persons or bodies to whom personal data, the profile or the result of the processing may be communicated as well as the right to object to it.

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

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

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

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

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

a. this is provided for by law, which lays down measures to safeguard data subjects' legitimate interests, particularly by allowing them to put forward their point of view;
b. the decision was taken in the course of the performance of a contract to which the data subject is party or for the implementation of pre-contractual measures taken at the request of the data subject and that measures for safeguarding the legitimate interests of the data subject are in place.

5.6. In any event, and not only in the cases referred to in Principle 5.5, when the profiling processing system issues a decision or a draft decision, it is recommended that:

a. the controllers consider all the particularities of the data and not only rely on decontextualized information or results of the processing;
b. in the event of high-risk processing operations, the controller sets up a service where a natural person will inform the data subject of the algorithmic operations underlying the data processing, including the consequences of these operations for him/her. In that case, the information must be such as to enable the data subject to understand the justification for the decisions or proposals for decisions regarding him/her;
c. in that case, the natural person appointed by the controller must be able, on the basis of reasonable arguments, to decide not to rely on the results of the recommendations resulting from the use of profiling processing;
d. where there are indications of direct or indirect discrimination based on the functioning of the profiling processing operation, controllers and processors shall provide evidence of the absence of discrimination.

5.7. Persons affected by a decision based on profiling processing have the right to challenge it in front of a competent authority.

5.8. Unless explicitly consented to, the data subject must be able to object by an easy means to the transfer or sharing of data either for profiling purposes by third parties or of the results of profiling processing.

## 6. Exceptions and restrictions

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

## 7. Remedies

7.1. Domestic law should provide appropriate sanctions and remedies in cases of breach of the relevant provisions of domestic law.

## 8. Data Security

### General provisions

8.1. Appropriate technical and organisational measures should be taken, in particular on the basis of the principles of 'privacy by design' and 'privacy by default', 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.

8.2. 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.

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

8.4. 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.

8.5. 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.

8.6. The controllers should assess the risk of re-identification taking into account the time, effort or resources required with regard to the nature of the data, the context of their use, the available re-identification techniques and the corresponding costs. Data controllers should demonstrate the adequacy of data anonymisation measures and guarantee the effectiveness of pseudonymisation or anonymisation; Technical measures may be combined with legal or contractual obligations in order to prevent any possible re-identification of the data subjects. Data controllers should regularly reassess the risk of re-identification, in view of technological advances in anonymisation techniques.

**Special provisions for profiling processing using automatic learning processes**

8.7. In order to ensure trust in AI systems, controllers and, where applicable, processors shall ensure the use of robust and safe systems, in particular with regard to the setting up of procedures in the event of breakdown, malfunction or error of the system. They shall ensure on a regular basis and throughout the life of the system that it is reliable and that its results are consistent with the model and reproducible.

8.8. Controllers and, where applicable, processors shall ensure a critical assessment of the quality, nature and quantity of the data used by eliminating unnecessary data and any data that could bias the results. They ensure the robustness of the model in case of new data input.

8.9. Controllers and, where applicable, processors shall ensure the transparency of the functioning of the systems and the traceability of the processing results. They will ensure that their intellectual property rights and trade secrets are only minimally opposed and, in no way will they be able to oppose the request of a data subject or of a group to be able to understand the decisions or proposed decisions taken from the profiling processing operations. Artificial intelligence applications should allow effective control of the effects of its applications on individuals, groups and society by both concerned data subjects and groups.

8.10. For the purposes of a continuous assessment of both individual and collective risks, and in any case when it comes to high-risk profiling processing operations, data controllers and, where appropriate, processors should surround themselves with a multidisciplinary assessment team and consult representatives of the interests involved in profiling. Such evaluation process should be conducted by qualified and adequately knowledgeable professionals who would assess the various impacts, including their legal, social, ethical and technical dimensions.

## 9. Supervisory authorities

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

9.2. Furthermore, in cases of processing that use profiling and entail special risks with regard to the protection of privacy and personal data, in particular in the case of high-risk processing operations and of profiling processing carried out by public authorities, member states may foresee either:

a. that controllers have to notify the supervisory authority in advance of the processing; or

b. that this processing is subject to prior checking by the supervisory authority.

9.3. In the implementation of this recommendation, supervisory authorities should cooperate as far as possible with consumer and competition protection authorities as well as with institutions responsible for equal opportunities or for the promotion of democracy.

9.4. When analysing profiling processing operations, the supervisory authorities must extend their competence to the analysis of collective risks and risks to the society. They will ensure that their opinions mention such risks and that their decisions take them into account. If necessary, they will provoke debates on the subject. They will draw the attention of member states on the importance of broadening their expertise in this field.

9.5. In this context, supervisory authorities should receive and investigate complaints from associations concerning the collective interest of a group or the general interest. If necessary, the authorities will make recommendations in this regard.

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

## 10. Additional measures

### The creation of an independent national authority for AI risk assessment

10.1. Without prejudice to the supervisory authorities' powers in the field of data protection, member states should set up an "independent multidisciplinary national authority to assess the risks associated with artificial intelligence and in particular with profiling processing using machine learning processes". Such an independent authority would be in charge of auditing, testing and labelling AI

systems in the private or public sectors. The intervention of this authority would be mandatory for AI used in public sector activities and, subject to what member states may decide on high-risk systems, be on a voluntary basis for systems operated by the private sector.

10.2. Such an authority would issue opinions on, firstly, any individual or collective profiling processing envisaged by administrations or the regulatory authority to support their strategies or apply regulations, and secondly, on the assessment of the risks associated with private or public policies in terms of 'data sharing' and 'open data' and support for the definition and implementation of 'good practices'.

10.3. That authority should issue recommendations on the quality of megadata and profiling algorithms in order to ensure their reliability, transparency and compliance with applicable legislation, in particular with regard to data protection, consumer protection, non-discrimination, competition, etc.

10.4. This authority would work in close cooperation with the supervisory authorities.

10.5. Its opinions and recommendations would be public.

**Labelling and certification of AI and data protection systems**

10.6. Member states and supervisory authorities should encourage the setting up of independent and qualified certification mechanisms for AI and data protection systems and related labels and marks to demonstrate that processing operations carried out by controllers and processors comply with this recommendation. The specific needs of both micro, small and medium-sized enterprises and different sectors should be taken into account.

10.7. Member states may lay down conditions for the approval of bodies which would set up the control mechanisms referred to in Principle 10.6.

10.8. Certification is voluntary and accessible through a transparent process. A certification under this Principle shall not reduce the liability of the controller or of the processor to comply with this recommendation or with applicable laws.

10.9. Data controllers and processors, whose systems are certified or labelled will affix the certification or label mark at least on their website and on the information for data subjects. They shall ensure that, via such a mark, access to the certificate or label is accessible to anybody.

**With regard to profiling processing operations carried out by public authorities**

10.10. The profiling processing operations carried out by public authorities both to define their strategies and to apply them must be based on a clear, proportionate and necessary law in a democratic society, according to the understanding of the case law of the Council of Europe.

10.11. In accordance with Principle 10.1., the design, development, implementation and monitoring of AI systems, in particular profiling systems, should be submitted to the independent multidisciplinary national authority for risk assessment of artificial intelligence.

10.12. The requirements for access to administrative documents and the reasons for public decisions require that computerised decision-making or decision-support systems be transparent and that citizens may, notwithstanding any technical or legal arguments, have access to the reasoning held by the algorithm.

10.13. Public authorities shall ensure that the requirements of these recommendations, in particular those specific to them, are communicated to their processors as part of their terms of reference.

**Provisions regarding research and education**

10.14. Member states should encourage, independent, interdisciplinary and open, including fundamental, research, in particular on the reliability, audibility, robustness and transparency of AI systems including by allocating resources

10.15. Member States should encourage open source initiatives for design and disseminating of algorithms.

10.16. Member States should allocate resources to multidisciplinary digital literacy at all levels of education in order to raise people's awareness of digital issues and, in particular, AI. They should likewise encourage professional training, training of administrations and business managers to the technical aspects and societal and human rights issues of the systems used in profiling, in particular through interdisciplinary courses to be included in education and post-graduation curricula for digital professions.