PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA IN THE CONTEXT OF PROFILING

Recommendation CM/Rec(2021)8

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA IN THE CONTEXT OF PROFILING

Recommendation CM/Rec(2021)8
adopted by the Committee of Ministers
of the Council of Europe
on 21 November 2020

Council of Europe

French edition:
Protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage

Cover and layout: Documents and Publications Production Department (DPDP), Council of Europe

Printed at the Council of Europe

Contents

Recommendation CM/Rec(2021)8

(Adopted by the Committee of Ministers on 3 November 2021 at the 1416th meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recalling that digital technologies allow the large-scale processing of data, including personal data, in both the public and private sectors, used for a wide range of purposes including for services widely accepted and valued by society and individuals;

Noting that data are processed in particular by calculation, comparison, correlation and other statistical techniques, with the aim of producing profiles or models that could be used in many ways for different purposes and uses, by matching the data of several individuals;

Considering that, by observing and linking a large amount of data, even anonymous data, profiling techniques can have an impact on the data subjects by placing them in predetermined categories, very often without their knowledge;

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 individuals' rights and freedoms;

Noting that the data processed in the context of profiling may include special categories of personal data, notably biometric data, the misuse of which can cause irreversible damage to data subjects, since such data can be used to access various services and can have legal consequences;

Considering in particular that the protection of fundamental rights, notably the rights to privacy and to protection of personal data, safeguards the existence of different and independent spheres of life where each individual can control his or her information;

Considering the particular vulnerability of some of the persons profiled, including children, and the possible seriousness of the consequences of such profiling, sometimes for the rest of their lives;

Aware of the intensification and diversification of the profiling of individuals, in all spheres of activity;

Having regard to the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108, hereafter "Convention 108"), as modernised by the Amending Protocol[1] (CETS No. 223), and convinced of the desirability of facilitating the application of those principles in the context of profiling;

Emphasising that member States should ensure compliance with applicable legislative and regulatory frameworks, and guarantee procedural, organisational and substantive safeguards and access to effective remedies with regard to all relevant actors, while promoting an environment in which technological innovation respects and enhances human rights and complies with the fundamental obligation that any restriction of human rights must be necessary and proportionate in a democratic society and implemented in accordance with the law;

Realising that the situation has considerably evolved since the adoption of Recommendation CM/Rec(2010)13 of the Committee of Ministers to member

1. The Protocol amending Convention 108 (CETS No. 223) was opened for signature on 10 October 2018 and the modernised convention has yet to enter into force. It is hereafter referred to as "Convention 108+".

States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, and that both the methods and the impact of profiling have radically changed;

Bearing in mind that digital technologies hold significant potential for innovation and growth, and that the achievement of these goals must be rooted in the shared values of democratic societies;

Noting that the rapid evolution of both the technologies used and the capacities of algorithms is accompanied by a constant increase in the volume of personal data processed, and that while paving the way for innovation and growth, this convergence of factors can also pose risks, at both the individual and collective levels;

Observing that those developments prompt the updating of Recommendation CM/Rec(2010)13, having due regard to Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems,

Recommends that the governments of member States:

- take into account the principles set forth in the appendix to this recommendation, which replaces the above-mentioned Recommendation CM/Rec(2010)13, in their law and practice;
- ensure that this recommendation and its appendix are translated and disseminated as widely as possible among competent authorities and stakeholders, including supervisory authorities, human rights organisations, civil society organisations and the private sector;
- promote acceptance and application of the principles set forth in the appendix to this recommendation by all stakeholders, ensuring that private-sector actors engaged in the design, development and deployment of profiling activities comply with the applicable laws and fulfil their responsibilities to respect human rights.

Appendix to Recommendation CM/Rec(2021)8

1. Definitions

1.1. For the purposes of the present recommendation:

a. "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, resources or effort in relation to the means at the disposal of the controller.

b. "Categories of data processed" means the different types of data used during the profiling processing, regardless of their source and nature.

c. "Profiling" refers to any form of automated processing of personal data, including use of machine learning systems, consisting in the use of data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

d. "Profile" refers to a set of data attributed to an individual, characterising a category of individuals or intended to be applied to an individual.

e. "Model" is a mathematical abstraction used, for example, in automatic learning methods, which provides a simplified description of the data to solve the task to be performed.

f. "Artificial intelligence" (AI) means a system that is either software-based or embedded in hardware devices, and that displays intelligent behaviour by, *inter alia,* collecting and processing data, analysing, and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals.

g. "Machine learning processing" means processing using particular methods of AI based on statistical approaches to give computers the ability to "learn" from data, that is, to improve their performance in solving tasks without being explicitly programmed for each of them.

h. "Automated decision-making system" refers to a system that uses automated reasoning to aid or replace a decision-making process that would otherwise be performed by humans.

i. "Online intermediary services" means information society services that enable users to receive information (online search services), goods or services or to establish relations (social network access service).

j. "High-risk profiling" may refer, inter alia, to:

i. profiling operations that entail legal effects or have a significant impact on the data subject or on the group of persons identified by the said profiling;

ii. profiling that – because of the target audience, the context or the purpose of profiling – especially in a situation of imbalance of information power, involves a risk of unduly affecting or influencing the data subjects, particularly in the case of minors and other vulnerable individuals;

iii. profiling that involves data qualified as special categories of data under Article 6 of Convention 108+ or that is aimed at detecting or predicting these data;

iv. profiling that affects a very large number of individuals, including profiling carried out by online intermediary services for their own use or that of a third party.

2. General principles

2.1. Respect for fundamental rights and freedoms, notably the rights to human dignity and to privacy but also to freedom of expression, and for the principle of non-discrimination and the imperatives of social justice, cultural diversity and democracy, should be guaranteed, in both the public and private sectors, during the profiling operations covered by this recommendation.

2.2. Profiling should contribute to, or at least not negatively impact, both the well-being of individuals and the development of an inclusive, democratic and sustainable society.

2.3. In the context of an increasing use of big data, both personal and non-personal data are collected. Furthermore, with automated processing, based in particular on the use of machine learning systems, it is difficult to know a priori which data will allow correlations or predictions to be made regarding a data subject. In such cases, for personal data to be processed fairly, organisations should ensure the relevance and quality of all data, including non-personal data, that could inform correlations or predictions about a data subject.

2.4. All automated decision systems are designed by humans and have some degree of human involvement in their operation. Humans are ultimately

responsible for how a system receives its inputs (for example, who collects the data that feed into a system), how the system is used, and how a system's outputs are interpreted and acted on. The systems (especially those based on AI) must allow operational human intervention whenever appropriate or necessary to ensure their legitimate functioning, including in respect of the principles of fairness and non-discrimination.

2.5. 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) and for the whole duration of data processing, notably through the use of privacy-enhancing technologies. They should also take appropriate measures to combat the development and use of technologies which are aimed, wholly or partly, at the illicit circumvention of technological measures protecting privacy.

2.6. Profiling must not result in discrimination against individuals, groups or communities. It must undermine neither the dignity of persons nor democracy. The use of automated decision-making systems should preserve the autonomy of human intervention in the decision-making process.

2.7. Profiling should not be carried out for the purpose of manipulating data subjects or the persons close to them, including in respect of their choices or opinions.

2.8. At least when the data subject's consent is required, service providers and, in particular, online intermediary services should give data subjects the possibility to opt in to profiling and to choose between the different profiling purposes or degrees. The data subject should be informed of all the consequences of his or her choice.

2.9. Member States should ensure that the legal framework applicable to profiling is such that the profiling remains proportionate to the purposes pursued, and to the nature and gravity of the risks incurred by the data subjects or the targeted groups. The specific needs of both micro, small and medium-sized enterprises and different sectors should be taken into account. If the profiling activities carried out are of a high-risk nature, the same level of strictness should be applied regardless of the size of the enterprise.

2.10. The use of automated decision-making systems based on AI technologies poses additional risks due to possible errors and biases, and the difficulty of making the justification for decisions taken and ensuring transparency, consequently impeding the full exercise of the rights of the data subjects. The design,

development and implementation of automated decision-making systems based on AI require special and continuous attention with regard to the risks created, and their assessment by multidisciplinary, independent teams.

2.11. Profiling involves different actors whose quality and role must be analysed in order to determine their potential joint responsibilities, especially in the case of data sharing.

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

A. Lawfulness

3.1. The processing of personal data in the context of profiling should be fair, lawful, proportionate, and for specified and legitimate purposes, and never be carried out in a way incompatible with such initial purposes. The processing of personal data for a compatible purpose in the context of profiling may only be performed if it is provided for by domestic law or is based on consent in accordance with principle 3.4, which stipulates specific appropriate safeguards with regard to these data.

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. In machine learning systems, it is difficult to know a priori which data will allow significant correlations. However, it is important to limit the profiling to categories of data that the data subject can reasonably expect (legitimate expectations) to be taken into account in view of the purposes of profiling.

3.3. Personal data used in the context of profiling should be at least 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 processed. If possible, for the purposes for which the data are processed, the data should be anonymised.

3.4. Except where stated below, processing of personal data in the context of profiling may only be performed:

- if it is explicitly provided for by domestic law, in order to safeguard the data subjects' rights and freedoms and their legitimate interests; or
- if the data subject or her or his legal representative has given her or his free, specific, informed and unambiguous consent. In the case of high-risk profiling, the consent ought to be explicit; or

– if the 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

– if it 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

– if 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 subject or in respect of the processing of special categories of data. The necessity should be explicitly substantiated by the controller; or

– if it is necessary to safeguard the vital interests of the data subject or of other persons.

3.5. When the profiling is based on consent, the processing of personal data in the context of profiling of persons who cannot express their free, specific, informed and unambiguous consent themselves should be forbidden, except when specific consent is given by the legal representative or when this processing is in the legitimate interest of the data subject, or if there is an overriding substantial public interest, on the condition that appropriate safeguards are provided for by law.

3.6. As far as possible, service providers and platforms should offer different services that are either more or less personalised, or non-personalised, depending on the service offered, in order to guarantee to the data subject a choice as regards the intensity of profiling. In order to be free, consent implies that the data subject has the possibility of an informed choice. Consent to profiling should not be required as a condition for the performance of a service. Where the profiling is based on consent, it is incumbent on the controller to prove that the data subject has agreed to the profiling beyond what was necessary for the performance of the service, on an informed basis, as set out in section 4 and in compliance with the requirements that consent should have under principle 3.4.

3.7. As far 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, without having to communicate personal data to the goods or services provider.

3.8. In order to ensure free, specific, informed and unambiguous consent to profiling, online intermediary services should ensure, by default, non-personalised access to information about their services.

3.9. The distribution and use, without the data subject's knowledge, of software aimed at the observation or 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 law, constitute a measure necessary and proportionate within a democratic society and are accompanied by appropriate safeguards.

B. Quality of data and algorithms

3.10. Appropriate measures should be taken by the controllers and, where applicable, the processors to correct data inaccuracy factors and limit the risks of errors and biases inherent in profiling.

3.11. The controllers 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, as well as the impact of the use of profiling on the data subject's rights.

3.12. When acquiring data or algorithms from a third party, the controller(s) or processor(s) should obtain from the third party the documentation necessary to check the quality of the data and algorithms and their relevance to the purpose of the processing.

C. Special categories of data

3.13. Processing of sensitive data defined under Article 6 of Convention 108+ in the context of profiling should only be allowed where appropriate safeguards are enshrined in law and the data are necessary for the lawful and specific purposes of the processing.

3.14. Processing for the purpose of detecting or predicting racial or ethnic origin, political opinions, trade union membership, religious or other beliefs, health or sexual life should be prohibited and should only be allowed where appropriate safeguards are enshrined in law and the data are strictly necessary for the lawful and specific purposes of the processing. When consent is required, it should be explicit where the processing concerns such data.

4. Information

4.1. Where personal data relating to a data subject are collected from the data subject in the context of profiling, the controller should, at the latest when the data are obtained, provide the data subject with the following information:

a. that their data will be used, or are intended to be used, in the context of profiling by the controller and/or by third parties;

b. the legal basis and the purposes for which the profiling is carried out;

c. the categories of data used in the context of the profiling;

d. the identity of the controller and his or her establishment or habitual residence and, if necessary, that of his or her representative;

e. the existence of appropriate safeguards where required, as is notably the case for special categories of data;

f. the categories of persons or bodies to whom or to which the personal data or the results of the profiling may be communicated, and the purposes for doing so;

g. the conditions of exercise of the right of access, objection, rectification or erasure, as provided for by principle 5 of this appendix, as well as the right to bring a complaint before the competent authorities;

h. all information that is necessary for guaranteeing the fairness of use of profiling, such as:

- the possibility, where appropriate, for the data subjects to refuse or withdraw consent and the consequences of withdrawal;
- the persons from whom or bodies from which other personal data are or will be collected;
- the compulsory or optional nature of the reply to the questions used to collect the data and the consequences for the data subjects of not replying;
- the duration of storage of the personal data;
- where applicable, the potential impact of the profiling on the data subject;
- meaningful information about the reasoning underlying the profiling or the model used by the data controller.

4.2. Where personal data have not been obtained from data subjects, the controller should provide them, at least in a general notice, with the information

listed in principle 4.1 as soon as the personal data are processed or, if it is planned to communicate these data to a third party, at the latest when the personal data are first communicated. In addition to the information listed in principle 4.1, the information should include the origin of the data collected, the legal basis for the data transmission or sharing and the possibility to object to this transmission or sharing.

4.3. The information provided to the data subject should be delivered in a comprehensible manner and adapted to the circumstances. When personal data are processed in the context of profiling, the controller could indicate the existence of a profiling activity with an icon. This icon should make it possible for anyone to automatically obtain the information listed under principle 4.1 by linking to the website of the controller.

4.4. Where personal data were previously collected with no intention of applying profiling methods and are subsequently processed lawfully in the context of profiling, the controller should have to provide the information foreseen under principles 4.1 and 4.2.

4.5. Principles 4.2, 4.3 and 4.4 on informing data subjects do not apply if the data subject has already been informed. Moreover, where personal data are not collected from the data subject, principles 4.2, 4.3 and 4.4 do not apply if:

a. it proves impossible to provide the information or it would involve disproportionate effort; or

b. the restrictions to the right of information are provided for by domestic law.

5. Data subjects' rights

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, whether they were used in a pseudonymised form or not, and any other necessary additional information to ensure fair and transparent processing (including anonymised data sets used in the processing) and, in the case of use of profiles, the data inferred by the use of the profiling system;

b. the reasoning underlying the processing of his or her personal data used to attribute a profile to him or her, at least in the case of an automated decision and, in the case of the use of processing based on machine learning,

information about the model used by the algorithm. In that case, the information provided must enable the data subject to understand the reasons for the decision or the proposed decision regarding him or her;

c. the purposes for which the profiling was carried out;

d. the categories of persons or bodies to which personal data, the profile or the result of the processing may be communicated, as well as the right to object to it;

e. the name and address of the person in charge of redress by the data subjects against a decision or draft decision, as prescribed under principle 5.8.

5.2. Data subjects should be entitled to obtain, without undue delay, erasure or rectification of their personal data, if the data are processed contrary to the principles of this recommendation, notably when using or predicting special categories of data without the appropriate safeguards prescribed by domestic law.

5.3. Except when the law provides for profiling and lays down measures to safeguard the data subject's legitimate interests, the data subject should be entitled to object to the processing of his or her personal data, at any time, on grounds concerning him or her. Unless the controller demonstrates legitimate grounds for the processing, which override the interests or fundamental rights and freedoms of the data subject, the profiling should no longer involve the use of his or her personal data. Where the purpose of the profiling is direct marketing, no justification should be requested from the data subject.

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 would negatively impact 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 the legitimate interests, rights and fundamental freedoms of the data subjects, particularly by allowing them to put forward their point of view;

b. the decision was needed to ensure the performance of a contract to which the data subject is party or to implement pre-contractual measures taken at the request of the data subject, and that measures to safeguard the legitimate interests, rights and fundamental freedoms of the data subject are in place.

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

a. the controller considers all the particularities of the data and does not simply rely on information or processing results taken out of context;

b. in the event of high-risk profiling, the controller informs the data subject of the algorithmic operations underlying the data processing, including the consequences of these operations for him or her. The information should be such as to enable the data subject to understand the justification for the decisions or draft decisions;

c. the person appointed by the controller is able, on the basis of reasonable arguments, to decide not to rely on the results of the recommendations arising from the use of profiling;

d. where there are indications of direct or indirect discrimination based on the functioning of the profiling operation, controllers and processors provide evidence of the absence of discrimination.

5.7. Persons affected by a decision based on profiling should have the right to receive a meaningful explanation of this decision or draft decision to understand the justification for it. Intellectual property or the existence of trade secrets may only be opposed where the information to be given would seriously affect these rights. The invocation of these rights and interests by the controller may not lead to deprive the data subject or the affected group of the capacity to understand the decisions or draft decisions taken by the controller.

5.8. Notwithstanding recourse before a supervisory authority or legal redress, data subjects should have the right to challenge the profiling before a person nominated by the data controller, who has access to all the information about the profiling and its functioning, and is qualified to modify or delete the decision or draft decision.

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

6. Exceptions and restrictions

6.1. Where it constitutes a necessary and proportionate measure in a democratic society for reasons of national security, defence, public safety, and other grounds listed in Article 11 of Convention 108+, the provisions set out in sections 3, 4 and 5 may be subject to restrictions. Such restrictions furthermore have to be provided for by law and respect the essence of the fundamental rights and freedoms, notably freedom of expression.

6.2. Provisions set out in sections 4 and 5 may be subject to restrictions according to Article 11.2 of Convention 108+ for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes, where there is no recognisable risk of infringement of the rights and fundamental freedoms of individuals.

7. Data Security

A. General provisions

7.1. 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 Convention 108+, to guard against accidental or unlawful destruction and accidental loss, as well as unauthorised access, alteration, communication or any other form of unlawful processing.

7.2. 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 processed in the context of profiling and the evaluation of the potential risks. They should be reviewed periodically and within a reasonable time.

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

7.4. If necessary, the controllers should appoint independent persons responsible for the security of information systems and data protection, and who are qualified to give advice on these matters.

7.5. 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.

7.6. In the case where data have been anonymised or pseudonymised, the controllers should assess the risk of re-identification of the data subject (taking into account in particular the time, effort or resources required with regard to the nature of the data, the context of their use, the re-identification techniques available and the corresponding costs). Controllers should demonstrate the adequacy of data pseudonymisation or anonymisation measures and guarantee their effectiveness. If there is a risk of re-identification of the data subject, such data can no longer be considered anonymised data. Technical measures may be combined with legal or contractual obligations in order to prevent any possible re-identification of the data subject. Controllers should regularly reassess the risk of re-identification, in view of technological advances in de-anonymisation techniques. Member States may regularly lay down a list of pseudonymisation and/or anonymisation techniques for controllers to use.

B. Special provisions for profiling based on AI systems using automatic learning processes

7.7. In order to ensure trust in AI systems and their lawfulness, controllers and, where applicable, processors should ensure the use of reliable and safe systems, in particular with regard to the setting up of procedures in the event of breakdown, errors or inconsistencies during the system's entire life cycle. They should 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. The system ought to be robust against attacks or other manipulation of the data or the algorithms.

7.8. Controllers and, where applicable, processors should ensure a critical assessment of the quality, representative nature and quantity of the data used, by eliminating unnecessary data and any data that could bias the results. In particular, specific thresholds of accuracy of results should be met. Controllers ensure the robustness of the model in case of new data input.

Results themselves should be assessed to evaluate their impact on the data subject, including with regard to the right to non-discrimination. AI applications should allow effective control, by the data subjects and groups concerned, of the effects of their applications on individuals, groups and society.

7.9. For the purposes of the ongoing assessment of both individual and collective risks – and in any event when it comes to high-risk profiling operations – controllers and, where appropriate, processors should document the training of the model and carry out regular impact assessments addressing the specific risks of profiling based on AI systems. To achieve this purpose, they should surround themselves with a multidisciplinary assessment team and consult representatives of the interests involved in the profiling, including the profiled people. Such an evaluation process should be conducted by qualified and knowledgeable professionals able to assess the various impacts, including their legal, social, ethical and technical dimensions.

8. Supervisory authorities

8.1. Supervisory authorities under Article 15 of Convention 108+ ensure compliance with the domestic law, implementing the principles set out in this recommendation.

8.2. Where the envisaged profiling activity is of a high-risk nature, member States may stipulate that controllers should notify its existence to the supervisory authority and, if requested by the latter, make available all the documents relating to the procedure followed, the evaluation itself and provide information about the corrective measures taken or envisaged.

8.3. Intellectual property or the existence of trade secrets cannot lead to the supervisory authority being deprived of the capacity to exercise its powers and, for example, to assess the automated decision making.

8.4. In the implementation of this recommendation, supervisory authorities should co-operate 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. Where an independent multidisciplinary national authority exists for assessing the risks associated with AI, and in particular with profiling using machine learning processes, the supervisory authority should co-ordinate its work with this institution.

8.5. The field of inquiry of supervisory authorities should be broadened to include collective and societal risks. Their opinions should mention such risks and their decisions should take them into consideration.

8.6. In this context, supervisory authorities should be entitled to receive and investigate complaints from associations concerning the collective interest of a group or the general interest, and where appropriate impose sanctions.

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

9. Additional measures

A. Labelling and certification of AI and data protection systems

9.1. Member States and supervisory authorities should encourage the setting up of independent and qualified certification mechanisms for AI systems as regards their compliance with legal requirements for data protection, in particular the training and resulting model on which profiling is based and related labels and trust marks, as an element to demonstrate that processing operations carried out by controllers and processors comply with this recommendation.

9.2. Member States may lay down conditions for the approval of bodies that would set up the supervisory mechanisms referred to under principles 8.1 and 8.2.

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

9.4. Data controllers and processors whose systems are certified or labelled will indicate the certification or label mark at least on their websites and in the information to be given to data subjects. They should ensure that, via such a mark, access to the certificate or label is accessible to anybody. The period of validity of the certification should be limited in time.

B. Profiling operations carried out by public authorities

9.5. Without prejudice to the other applicable principles of the present recommendation, profiling operations carried out by public authorities should be lawful, proportionate and necessary in relation to the purposes of these operations.

9.6. The profiling operations carried out by public authorities, using automated decision-making systems either to define their strategies or to apply them, must be based on domestic law (clear, foreseeable and accessible), pursue a legitimate aim and be limited to what is necessary and proportionate to achieve that legitimate aim, taking fully into consideration all fundamental rights necessary in a democratic society, in accordance with the interpretation of the case law of the European Court of Human Rights.

9.7. The design, development, implementation and monitoring of AI systems, in particular profiling systems, should be submitted to the competent authority for the assessment of risks related to AI.

9.8. Public authorities should publish information on the reasoning underlying the processing or, in the case of the use of processing based on machine learning, an explanation in plain language of the model on which the system is based.

9.9. The individual decisions or draft decisions taken by public authorities and based on automated decision making systems should be transparent. Individuals and legitimate associations should, notwithstanding any technical or legal arguments, have access to the reasoning underlying the processing or, in the case of the use of processing based on machine learning, an explanation in plain language of the decision taken by the model on which the system is based. Without this, effective legal protection against the decisions would not be guaranteed.

9.10. Public authorities should 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.

C. Provisions regarding research and education

9.11. Member States should encourage independent, interdisciplinary and open research, including fundamental research, in particular on the reliability, auditability, robustness and transparency of AI systems, and allocate resources for this purpose. When relevant, that research should be led in dialogue with civil society representatives.

9.12. Member States should encourage open-source initiatives for the design and free dissemination of algorithms.

9.13. Member States should allocate resources to multidisciplinary digital literacy at all levels of education in order to raise people's awareness of the impact of profiling and AI on fundamental rights. They should likewise encourage professional training, including of administration and business managers, on the technical aspects and societal and human rights issues of the systems used in the context of profiling. Interdisciplinary courses should notably be offered in education and post-graduate curricula for IT professions.

In the last decade, profiling techniques have radically evolved, notably with the introduction of artificial intelligence and the use of machine learning systems. If these techniques can have benefits in the everyday life, they can impact individuals by placing them in predetermined categories, very often without their knowledge. This lack of transparency can pose significant risks to human rights, particularly for vulnerable persons, including children.

This recommendation, which updates a 2010 recommendation on the same topic, aims to align its provisions with the modernised data protection "Convention 108", known as "Convention 108+". It provides that respect for fundamental rights and freedoms, notably human dignity, privacy, freedom of expression, non-discrimination, social justice, cultural diversity and democracy should be guaranteed in both the public and private sectors during all profiling operations.

PREMS 159521

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE