**Submission by the Data Protection Unit of the Council of Europe to the OHCHR for the preparation of the thematic report on "the right to privacy in the digital age"**

The present submission is to inform the report by the United Nations High Commissioner for Human Rights on the right to privacy in the digital age that is going to be submitted to the Human Rights Council at its forty-fifth session pursuant to paragraph 10 of its resolution 42/15 adopted on 26 September 2019 ([A/HRC/RES/42/15](https://undocs.org/A/HRC/RES/42/15)).

The Data Protection Unit of the Council of Europe expresses its gratitude to the Office of the High Commissioner for Human Rights for the invitation to the expert seminar organised on 27 and 28 May 2020 which has discussed how artificial intelligence (AI) affects the enjoyment of the right to privacy and the articulation of safeguards necessary to promote and protect the right to privacy in the digital age.

To facilitate and enable that the European Convention on Human Rights applies both offline and online the Council of Europe has been developing high level and practical standards in binding and non-binding instruments which could enable states to commit to the respect, protection and promotion of these rights in the digital era. Fully aware of the potential and benefits that the internet, digitalization and new technologies, including AI could bring to the digital transformation of our societies, to the development of inclusive and global economies, to the preservation of our environment and *in fine* to the accomplishment of UN Sustainable Development Goals, the Council of Europe was always at the forefront of promoting changes undertaken in line with its core values and objectives: human rights, rule of law and democracy.

**General legal framework (relevance of Convention 108/+)**

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) is the only legally binding multilateral instrument in the area of protection of privacy and personal data which has been open for signature in 1981. Since then, it has influenced various international (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), regional (EU, African Union) and national privacy legislations. Convention 108 through its 55 parties and 32 observers expands on all continents and provides for a principle-based framework for the protection of individuals’ privacy and personal data and a viable forum for cooperation to supervisory authorities. As being recently modernised by the Protocol CETS No. 223 (Convention 108+) it will ensure, upon its entry into force in the coming years, that the free flow of data is facilitated, including to and from the European Union and the respect for human dignity in the digital age is secured. Its Conventional Committee with its 70-80 members and observers will continue to offer a unique forum for discussions and deliberations concerning the rights to privacy and data protection at multilateral level and in the meantime a viable legal instrument for the convergence towards a high set of standards globally.

Parties to Convention 108 have already reaffirmed several times that Convention 108+, based on its personal and material scope can be applicable to all data processing involving personal data even if carried out by new data processing techniques and technologies, such as big data analytics, artificial intelligence, machine learning, profiling, facial recognition, etc. Albeit not greatly detailed on every instances – on purpose to allow different legal systems and jurisdiction to adhere to it – Convention 108+’s provisions could give enough reassurance to a country and to individuals to address the concerns they might have in relation to the application of new data processing techniques and technologies in both public and private sector. These might include its provisions on overarching and high level data protection principles, related to the legitimacy of data processing, such as the proportionality and necessity, the principle of processing personal data on valid legal basis, for explicit, specified legitimate purposes and to the quality of data (Article 5), special categories of data (Article 6), data security (Article 7), transparency (Article 8), accountability measures such as privacy by design, data protection impact assessments (Article 10), new generation of data subject’s rights such as the right not to be subject to a decision based solely on automated processing, right to know the reasoning of the processing, right to object (Article 9), its state-of-the art exception (Article 11) and cross-border data flow regimes (Article 14) and the requirements for stronger powers, resources for data protection authorities (Chapter IV) with a forward-looking obligation to cooperate in transnational cases (Article 17). Building on the effective and efficient implementation of these underpinned by new powers and functions of its Conventional Committee (Article 4, paragraph 3 and in Article 23, litterae e, f and h) and on the prospect that other UN Member States also wishes to accede to Convention 108+ Convention 108+ has the promise of becoming a global benchmark in the area of the protection of privacy and personal data in the digital age.

**Recommendations on the use of algorithms**

The Council of Europe’s work in the field of AI has been aiming at preventing abuses of algorithmic systems and processes and at contributing to building a doctrine of use that can guarantee effective protection of all human rights. Regulatory response to these issues remains highly placed on the Council of Europe’s agenda. [The Recommendation of the Council of Europe Committee of Ministers on human rights impacts of algorithm systems (2020/1)](https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154) (“Recommendation”) addresses human rights impact of AI technologies with guidance on obligations of states and responsibilities of companies.

The Recommendation urges the use of a precautionary approach - while using a broad definition of AI - to the development and use of algorithmic systems and the adoption of legislation, policies and practices that fully respect human rights. It calls on governments to ensure that they do not breach human rights, including the rights to privacy and to the protection of personal data through their own use, development or procurement of algorithmic systems. It stresses the need for the maintenance of accurate representations of data and a predictable legislative, regulatory and supervisory framework that prevent, detect, prohibit and remedy human rights violations, whether stemming from public or private actors, while also providing a set of “analysis and modelling” recommendations. Clear and strong requirements on transparency and accountability are equally empathised as core contributors to the acceptability, thus efficiency and effectiveness of those system and the availability of effective remedies is seen as a *sine qua non* condition for the necessary trust and confidence.

To ensure the full exercise of human rights and democratic freedoms a “*cooperation among states and with all relevant stakeholders, including civil society*’’ appears to be inevitable just as the development of democratic participation and awareness schemes and programmes.

It seems also to be of high relevance that while dealing with algorithmic systems states prioritise the inculcation of public and private expertise in the subject area, promote the importance and necessity of digital literacy, and take into account any environmental impact of large-scale digital services. They are called upon to strive towards creating sustainable models with optimised use of energy and natural resources.

The Recommendations also provides advices for the private sector in view of determining each actor’s responsibilities with respect to human rights and fundamental freedoms in the context of algorithmic systems. The private sector is recommended investing their efforts into developing systems that eliminate biases and discriminations that amount to violations of human rights and ensure transparency and accountability towards consumers in the creation of goods and services that utilise these systems.

At the same time, the Recommendation warns of significant challenges to human rights related to the use of algorithmic systems, mostly concerning the right to a fair trial; privacy and data protection; freedom of thought, conscience and religion; the freedoms of expression and assembly; the right to equal treatment; and economic and social rights.

**Data protection and Profiling**

Digital technologies can significantly contribute to innovation and growth, but it seems to be important that the achievement of these goals must be rooted in the shared values of democratic societies. This could prove to be challenging sometimes as rapid evolution of technologies used and the capacities of algorithms used along a constant increase of the volume of personal data processed can also cause risks at both the individual and collective levels. Among other factors these led to the update of the [Recommendation CM/Rec(2010) 13 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling](https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00) (“ [draft Recommendation on profiling](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cdd00)”) which is still pending the Committee of Ministers’ adoption. Using a broad definition for describing which activities can constitute profiling the draft Recommendation on profiling underlines the necessity for “*respect for fundamental rights and freedoms, notably the rights to human dignity and to privacy but also the freedom of expression and the principle of non-discrimination, but also the imperatives of social justice, cultural diversity and democracy, should be guaranteed during the processing of personal data, in both the public and private sectors*”.

To ensure the highest quality of data is key to every data basis and every data processing but it was found that for profiling activities in order to the personal data is processed fairly data controllers “*should ensure the relevance and quality of all data including non-personal data that could inform the correlation or prediction about a data subject*” as 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. As a general consideration the draft Recommendation calls on states to promote and to make legally binding the use of “*privacy by design*” approach during the whole duration of the processing 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.

In relation to transparency and data subject rights’ related requirements it is to be noted that “*The design, development and implementation of automated decision-making systems based on artificial intelligence require special and continuous attention with regard to the risks created and their assessment by multidisciplinary, independent teams*”. It seems furthermore recommendable in relation to those systems that the choice of a valid legal basis for the processing of personal data and purpose limitation settings are carefully designed (and lawful alternatives are present where the primary basis is consent) and that the proportionality of the system is measured against its intended purpose and the nature and gravity of potential risks.

It also needs to be stressed that 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 only be allowed where appropriate safeguards are enshrined in law and the data are strictly necessary for the lawful and specific purposes of processing.

In case their data undergo profiling data subjects shall have the right to receive a meaningful explanation of the decision to understand the justification for the decisions or proposals for decisions, in which intellectual property rights and trade secrets might only be evoked where the information to be given would seriously affect these rights and interests. It should in any case lead to depriving the data subject or the affected group of the capacity to understand the decisions or the draft decisions taken by the controller.

When it comes to data security a state-of-the-art solution should be sought that matches the sensitive nature of the personal data processed in the context of profiling and is able to mitigate the potential risks. Controllers moreover should demonstrate the adequacy of data pseudonymisation or anonymisation measures and guarantee their effectiveness. It is advisable that contingency plans are drawn up and the system is designed to be robust enough against attacks or other manipulation of the data or the algorithms.

Setting up multidisciplinary teams and organising consultations with representatives of interests’ groups involved in profiling, including profiled people is recommended through which the assessment of various impacts, including their legal, social, ethical and technical dimensions are secured.

It seems to be of high relevance that data controllers when informing data subjects on the data processing covers also possible risks as well as modalities and ways of exercising data subject rights, including the right to redress. If a data subjects exercises his/her right to object in direct marketing related data processing, there should not be any assessment carried out to balance his/her right with the legitimate interest of the data controller, but data subject’s wish need to be respected.

Supervisory authorities’ enhanced and multidisciplinary cooperation seems to be facilitated and the field of inquiry of supervisory authorities should be broadened to include collective and societal risks. States could also consider developing and rolling out programmes for labelling and certifying of AI and data protection systems and should ensure that when public authorities using profiling techniques that they are compliant with Article 11 of Convention 108+. Independent, interdisciplinary, including fundamental research, open source initiatives for design and free dissemination of algorithms should also be encouraged and 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, including the impact on fundamental rights of profiling and AI.

**Specific guidelines of possible relevance**

The Committee of Convention 108 has always felt necessary to issue specific guidelines which lay out in greater details the rights and obligations stemming from the provisions of Convention 108+ in one particular sector or for one particular type of data processing Three of its latest guidelines could be relevant for the purpose of the thematic report on "the right to privacy in the digital age":  [Guidelines on Artificial Intelligence and Data Protection](https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8), [Guidelines on Children’s Data Protection in an Education setting](https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b) and [Guidelines on facial recognition.](http://rm.coe.int/guidelines-on-facial-recognition/1680a134f3)

Guidelines on Artificial Intelligence and Data Protection

As a general principle it has to be stressed that the protection of human dignity and safeguarding of human rights and fundamental freedoms, in particular the right to the protection of personal data are crucially important when AI applications are used in decision-making processes. Any AI development relying on the processing of personal data should be based on the principles of Convention 108+ and key elements of this approach would imply to align the processing with requirements on lawfulness, fairness, purpose specification, proportionality of data processing, privacy-by-design and by default, accountability, transparency, data security and risk management. For AI, a risk based approach which aims at avoiding and mitigating the potential risks seems the be preferable (as opposed to the harm based approaches), where a wider view which considers not only human rights and fundamental freedoms but also the functioning of democracies and social and ethical values of the possible outcomes of data processing should be adopted. Data subject rights should guarantee a meaningful control by data subjects over the data processing and related effects on individuals and on society.

Developers, manufacturers and service providers should apply a values-oriented and at the same time precautionary approach in the design of their products and services which also takes duly into account the possible adverse consequences of AI applications on human rights and fundamental freedoms and involves appropriate measures for mitigating risks. A human rights by-design approach should be followed from as early as possible and any potential biases, including unintentional or hidden, and the risk of discrimination or other adverse impacts on the human rights and fundamental freedoms of data subjects should be avoided.

To ensure data quality unnecessary, redundant or marginal data during the development, and training phases should be reduced and then the model’s accuracy as it is fed with new data should be constantly monitored. The risk of adverse impacts on individuals and society due to de-contextualised data and de-contextualised algorithmic models may be considered, therefore the use of synthetic data should be preferred.

Consultation of external bodies (committees of experts, academic institutions) as well as participatory forms of risk assessment should be the norm, whereas every individuals shall be given the right not to be subject to a decision significantly affecting him/her based solely on automated processing, without having his/her views taken into consideration. It seems to be equally important that users’ freedom of choice over the use of AI, by providing feasible alternatives to AI applications should be guaranteed and forms of algorithm vigilance (specific duties on transparency, prior assessment of the impact of data processing on human rights and fundamental freedoms) that promote the accountability is to be adopted.

Data subjects should be informed if they interact with an AI application and have to have the right to obtain information on the reasoning, including also the consequences of underlying AI data processing operations applied to them. The right to object needs be ensured in relation to processing based on technologies that influence the opinions and personal development of individuals.

Legislators and policy makers should be encouraged to follow closely the principle of accountability, consider the adoption of risk assessment procedures and the application of other suitable measures, such as codes of conduct and certification mechanisms. To ensure transparency and human rights compliance, algorithm vigilance should be applied during public procurement procedures, whereas supervisory authorities must be sufficiently empowered to support and monitor the algorithm vigilance programmes

Guidelines on Children’s Data Protection in an Education setting

The guidelines suggest that profiling of children should be prohibited by law. In exceptional circumstances, states may lift this restriction when it is in the best interests of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law. Children’s attainment and achievement should not be routinely profiled to measure systems, for example, for measuring school or teacher performance management on the basis that this is not justified as an overriding public interest.

Recognition of the rights of the child, as the data subject, and their legal guardians, is both necessary in an algorithmic decision-making context, associated with processing personal data using artificial intelligence and informed processing.

Data protection and privacy impact assessments should have regard for the specific impact on children's rights and should demonstrate that the outcomes of algorithmic applications are in the best interests of the child and ensure that a child's development is not unduly influenced in opaque ways.

Predictions about groups or persons with shared characteristics based on analysis of large sets of personal data, shall still be considered as processing personal data, even where there is no intention for it to result in an intervention with an individual.

The distribution and use of software or use of services designed to observe and monitor user activity on a terminal or communication network building a profile of behaviour should not be permitted, unless expressly provided for by domestic law, and accompanied by appropriate safeguards.

Guidelines on facial recognition

Facial recognition is a processing of biometric data which shall only be allowed with an appropriate legal basis and additional guarantees provided for by law (in line with Article 6 Convention 108+).

The guidelines stress that certain uses of facial recognition technologies should be banned, in order to avoid any risk of discrimination. The use of facial recognition for the sole purpose of determining a person’s skin colour, religious or other belief, sex, racial or ethnic origin, age, health or social condition, unless appropriate safeguards are provided by law is suggested to be banned. This ban should also be applied to affect recognition technologies, which can identify emotions and be used to detect personality traits, inner feelings, mental health or workers’ engagement, since they pose important risks in fields such as employment, access to insurance or education.

It should be considered that the use of live facial recognition technologies in uncontrolled environments, in light of the intrusiveness it bares upon the right to privacy and the dignity of individuals, coupled with a risk of adverse impact on other human rights and fundamental freedoms, should be subject to a democratic debate on its use and the possibility of a moratorium pending complete analysis.

Developers, manufacturers and service providers should ensure the a) quality of data and algorithms, b) the reliability of the tools used, c) data security and d) are invited to educate users. It has to be recalled that entities using facial recognition technologies are subject to compliance with the principles and provisions applicable in terms of data protection
(legitimacy of the processing, requirements related to the processing of sensitive data, transparency, fairness, data quality, data security, transparency, accountability, minimisation, limited retention period, privacy impact analysis, privacy-by-design).

The rights of individuals must be guaranteed which should extend to request of rectification in case of false matches.

**Other related areas**

CAHAI

Council of Europe Ministers met in May 2019 in Helsinki and agreed to examine the feasibility and potential elements of a legal framework for the design, development and deployment of AI in line with Council of Europe standards of human rights, democracy and the rule of law.

An intergovernmental Ad Hoc Committee on Artificial Intelligence (CAHAI) has been established in the meantime for a two-year mandate. The task of the CAHAI is to examine the feasibility and potential elements of a legal framework (possibly binding) for the development, design and application of artificial intelligence, based on Council of Europe's standards on human rights, the Rule of Law and Democracy.

The creation of the CAHAI demonstrates the willing of Council of Europe’s member States to go beyond ethics. It is important to ensure member States’ compliance with their obligations under the European Convention on Human Rights. In this regard, it is worth recalling that the European Court of Human Rights holds member States accountable for the conduct of the private actors and therefore such States have the duty to create conditions that are conducive to the respect for human rights by such actors. Moreover, laying the foundations of a legal framework can also be an element of security for businesses.

The main elements of the feasibility study are already identified: a mapping of legally binding and non-binding legal frameworks on AI, as well as of risks and opportunities arising from the development, design and application of artificial intelligence (including human rights impact) shall be carried out with a view to detecting possible gaps. This will allow in turn identifying applicable principles to the design, development and application of AI.

Attention will be paid to coordinating with existing or ongoing work with other international organisations, in particular the European Union and the OECD, in order to promote synergies and avoid any duplication.

The working methods of the CAHAI will be transparent and open to inputs from civil society and observers, in compliance with the obligation to perform a broad multi-stakeholder consultation clearly set out in the CAHAI Terms of Reference. In this respect, it is worth noting that several requests of observer status to the CAHAI have reached the Secretariat, including from new companies or private sector’s actors wishing to sign a partnership agreement with the Council of Europe.

Surveillance

The protection of privacy is a universal human right which is guaranteed by article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. At regional level this right is enshrined in Article 8 of the European Convention on Human Rights (“ECHR”). The right to privacy is however not absolute right and can be lawfully restricted as Article 8.2 of the ECHR also suggests. This however cannot amount to compromising or breaching the very essence of this right. It is thus suggested that a narrow scope for exceptions and strict conditions along with a number of safeguards is proposed. Article 11 of Convention 108+ lays down a set of conditions and foresees safeguards to be put in place for data processing carried out for a rather restricted list of purposes and aims at ensuring that any interferences is permissible and deemed as lawful in a democratic society. The Committee of Convention 108 is currently working on a Guidance Note on art 11 to suggest even more clarity and details of the conditions and safeguards, but for the sake of the preparation of the thematic report on "the right to privacy in the digital age" the following cases from the European Court of Human Rights related to the state surveillance of communications could also be relevant: the case of *Malone v. The United Kingdom* as to the “*foreseeability of measures”*, the case of *Huvig & Kruslin v France* as to the “*sufficiently clear nature of the underlying legislation”*, the case of *Weber & Saravia v Germany “with respect to minimum safeguards”* and the cases of *Zakharov v Russia* and *Szabo v Hungary* as regards “*reasonable suspicion*”, “*strict necessity*” and “*judicial authorisation*”.

Covid-19

In order to assist Parties to Convention 108 in addressing privacy and data protection issues when setting up and implementing measures in view of the fight against the Covid-19 pandemic two joint declarations by the Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe have been published which recalled that general principles and rules of data protection are fully compatible and reconcilable with other fundamental rights and relevant public interests, such as public health and that it is essential to ensure that data protection frameworks continue to protect individuals and that the necessary privacy and data protection safeguards are incorporated in extraordinary measures that are taken to protect public health.

According to the first [Joint-Statement on the right to data protection in the context of the COVID-19 pandemic](https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter) (published on 30 March 2020) States must only take temporary measures that are necessary and proportionate to the legitimate aim pursued and which respect democracy, the rule of law and human rights, including the rights to privacy and to protection of personal data. The Joint Statement also highlights that particular attention is required in certain sectors concerned (public health, employment, telecommunications and education) and suggests concrete solutions which respect the applicable principles and rules.

The second [Joint Statement on Digital Contact Tracing](https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7) (published on 28 April 2020) “large-scale personal data processing can only be performed when, on the basis of scientific evidence, the potential public health benefits of such digital epidemic surveillance (e.g. contact tracking), including their accuracy, override the benefits of other alternative solutions which would be less intrusive”. There is a high need that these measures constitute an integral part of a national epidemiologic strategy, and the importance of the choice of the tracing model and its inclusive nature needs to be highlighted. The Joint Statement also establishes conditions of acceptability (acceptability which is also one of the conditions for the effectiveness) of such a system, among which trust and voluntariness are first and foremost. As for the legitimacy of the data processing, it advocates for a legal basis directly provided for by law, while keeping the voluntariness in the use of the application. Carrying out of a privacy impact assessment and the privacy-by-design principle figure among the guarantees to be used in relation to such processing operations. The necessity to thoroughly apply the purpose specification principle is highlighted and that practical applicability of important concepts are presented (such as the sensitivity, quality, minimisation of data, the right of data subjects with respect to automated decision-making, the necessity for de-identification of data, data security requirements, the link between the choice of digital architecture used and the protection of privacy, the importance of interoperability, transparency, temporary nature of databases, oversight and audit).

The Data Protection Unit of the Council of Europe *published a* report entitled “[*Digital solutions to fight COVID-19*](https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c)” on 12 October 2020 which deals with the issue of how personal data are processed in the 55 State Parties of Convention 108 in relation to the crisis caused by COVID-19. The report showcases commendable practices that have been followed by Parties, such as the use of privacy impact assessment and privacy by design principles in the shaping and implementation of digital solutions to support public health measures and those that needed to be improved, for example the mandatory use of contact tracing app for the whole population or measures taken in a state of emergency without time limit.

The Committee of Convention 108 issued also a statement on “[Covid-19 vaccination, attestations and data protection](https://rm.coe.int/t-pd-bur-2021-6rev2-statement/1680a25713)” in which it acknowledges the usefulness of means such as “vaccination passes” that are considered or already developed by some States, as well as the legitimacy of people’s wish to gain back some of the freedoms that were restricted due to the Covid-19 pandemic and the needs for the economy. It should be nevertheless recalled that health related data are sensitive data which requires additional guarantees when processed and no discrimination can be justified based on the fact that a person has not been vaccinated whatever the reason. It is also suggested that alternatives to the use of such digital tools need to be made available, and that their use cannot be made mandatory. Finally, it needs to be underscored that when setting up data base for the monitoring of the organisation of vaccination campaigns for instance strict respect to data protection principles and rules need to be observed.