**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)

**Other documents of possible interest**

On AI:

[Work of the Ad hoc Committee on Artificial Intelligence](https://www.coe.int/en/web/artificial-intelligence/cahai)

On surveillance:

Article 11 of Convention 108+

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*”

On Covid19:

[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)

[Joint Statement on Digital Contact Tracing](https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7)

[Digital solutions to fight COVID-19](https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c)

[Covid-19 vaccination, attestations and data protection](https://rm.coe.int/t-pd-bur-2021-6rev2-statement/1680a25713)