**EU contribution to the OHCHR report on the right to privacy in the digital age and Artificial Intelligence pursuant to Human Rights Council Resolution 42/15 on the right to privacy in the digital age**

**Introduction**

The European Union would like to thank the OHCHR for the call for contributions to the upcoming report regarding Human Rights Council Resolution 42/15 on the right to privacy in the digital age**.** The contribution from the European Union is comprised of both EU internal and EU external actions and policies (with thanks to DG CNECT, DG JUST and EEAS). As recommended, some of the questions were used as guidance to structure the final answer, which focuses on presenting details of the EU legislative proposal to regulate AI.

**EU’s contribution**

Artificial intelligence (AI) is a fast evolving family of technologies that can contribute to a wide array of economic and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of artificial intelligence can provide key competitive advantages to companies and support socially and environmentally beneficial outcomes, for example in healthcare, farming, education and training, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, and climate change mitigation and adaptation. At the same time, depending on the circumstances regarding its specific application and use, artificial intelligence may generate risks and cause harm to public interests and rights that are protected by Union law. Such harm might be material or immaterial.

Aside from the many beneficial uses of artificial intelligence, that technology can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and should be prohibited because they contradict international values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of the child.

AI can be deployed for malicious purposes, such as surveillance and censorship. Existing social patterns of bias and discrimination, e.g. on the basis of gender and/or race, can be perpetuated: when automation is based on biased data or algorithms, and there is a lack of diversity among those designing the technology. Privacy concerns are also pronounced as AI feeds on large amounts of data. The more AI is used for decision making, the higher the likelihood of opaque automation (“black boxes”), making it difficult to ensure the legality and/or ethicality of these processes.

For the EU, it is essential to join forces internationally to ensure that AI is developed and used within an ecosystem of excellence and trust, in line with international human rights law standards. The EU firmly defends that human rights apply both online and offline. The same rights, whether political, civil, economic, social or cultural, must be protected online.

Addressing the impact of AI on human rights requires a multi-stakeholder approach to policy-making: civil society, human rights defenders, national authorities, academia, international organisations and the private sector have to join efforts in identifying common solutions

**European legislative and regulatory frameworks**

On 21 April 2021, the Commission presented a proposal for a Regulation on a European

Approach for Artificial Intelligence.

The objective is the protection of fundamental rights and safety where AI is used, and

it includes provisions to enhance the effective enforcement of EU rules.

The proposal follows a risk-based approach. The EU identified high risks in areas such as

education, employment, access to credits or public assistance benefits, law

enforcement, migration and asylum, as well as the justice systems and remote biometrics

systems like facial recognition applications.

The EU already has rules protecting fundamental rights. But certain ‘black box’ AI

applications are complex and opaque, which can be a challenge.

The proposal will help to ensure that high-risk AI systems are designed in a fundamental

rights compliant way and the new requirements will ensure that possible breaches of

fundamental rights obligations can be investigated and addressed by national authorities

and courts.

To achieve this, the proposal includes requirements to ensure appropriate documentation

and testing of high-risk AI applications, as well as adequate human oversight and

reliability and accuracy of the systems.

The users of AI systems are the ones who need to respect fundamental rights, so they need

adequate information from the providers to ensure suitable use of their applications.

This is regulated in the proposal.

The regulation also empowers supervisory authorities that are in charge of fundamental

rights enforcement. Where an AI application falls in their mandate, they shall have access

to all documentation about that application, and they can team up with market surveillance

authorities to test AI systems that fall in their remit.

In addition to the proposal, we worked with the Member States on aspects like investments,

coordination of research and fostering skills under the “Coordinated Plan on AI”. An

update of this plan was presented jointly with the regulatory proposal.

The new AI legislation, builds on existing EU initiatives, taken over the past years:

For years, the Commission has been facilitating and enhancing cooperation on AI across the EU to boost its competitiveness and ensure trust based on EU values.

Following the publication of the [European Strategy on AI](https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF) in 2018 and after extensive stakeholder consultation, the High-Level Expert Group on Artificial Intelligence (HLEG) developed [Guidelines for Trustworthy AI in 2019](https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence), and an Assessment List for Trustworthy AI in 2020. In parallel, the first [Coordinated Plan on AI](http://europa.eu/rapid/press-release_IP-18-6689_en.htm) was published in December 2018 as a joint commitment with Member States.

The Commission's [White Paper on AI](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en), published in 2020, set out a clear vision for AI in Europe: an ecosystem of excellence and trust, setting the scene for today's proposal. The [public consultation](https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence) on the White Paper on AI elicited widespread participation from across the world. The White Paper was accompanied by a ‘[Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics](https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en)' concluding that the current product safety legislation contains a number of gaps that needed to be addressed, notably in the Machinery Directive.

EU’s participation on international efforts to Regulate AI

The EU participates, as an observer, to the process of development of the UNESCO Recommendation on the ethics of AI, which is scheduled to be approved at the General Conference in November 2021. The UNESCO standard setting instrument will prospectively tackle several policy areas, among which: ethical governance, data policy, development and international cooperation, environment and ecosystems, gender, culture, education, economy and labour, health etc. The EU and the EUMS have developed specific common lines on: the importance of full compliance with international law, in particular human rights law; the importance of striking the right balance between risks and benefits; gender equality; monitoring and evaluation – especially with a view to the fast evolving nature of AI.

The EU also works closely with the OECD and the Council of Europe on AI regulation.

 Further details of the EU legislation proposal

The new EU legislation will be applied directly in the same way across all Member States based on a future-proof definition of AI. They follow a risk-based approach:

**Unacceptable risk:** AI systems considered a clear threat to the safety, livelihoods and rights of people **will be banned**. This includes AI systems or applications that manipulate human behaviour to circumvent users' free will (e.g. toys using voice assistance encouraging dangerous behaviour of minors) and systems that allow ‘social scoring' by governments.

**High-risk:** AI systems identified as high-risk include AI technology used in:

* **Critical infrastructures** (e.g. transport), that could put the life and health of citizens at risk;
* **Educational or vocational training**, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
* **Safety components of products** (e.g. AI application in robot-assisted surgery);
* **Employment, workers management and access to self-employment** (e.g. CV-sorting software for recruitment procedures);
* **Essential private and public services**(e.g. credit scoring denying citizens opportunity to obtain a loan);
* **Law enforcement** that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence);
* **Migration, asylum and border control** **management** (e.g. verification of authenticity of travel documents);
* **Administration of justice**and**democratic processes** (e.g. applying the law to a concrete set of facts).

High-risk AI systems will be subject to**strict obligations**before they can be put on the market:

* **Adequate risk assessment and mitigation systems;**
* **High quality of the datasets** feeding the system to minimise risks and discriminatory outcomes;
* **Logging of activity to ensure traceability of results**;
* **Detailed documentation** providing all information necessary on the system and its purpose for authorities to assess its compliance;
* **Clear and adequate information** to the user;
* **Appropriate human oversight**measures to minimise risk;
* High level of **robustness**, **security** and **accuracy**.

In particular, **all remote biometric identification**systems are considered high risk and subject to strict requirements. Their live use in publicly accessible spaces for law enforcement purposes is prohibited in principle. Narrow exceptions are strictly defined and regulated (such as where strictly necessary to search for a missing child, to prevent a specific and imminent terrorist threat or to detect, locate, identify or prosecute a perpetrator or suspect of a serious criminal offence). Such use is subject to authorisation by a judicial or other independent body and to appropriate limits in time, geographic reach and the data bases searched.

**Limited risk**, i.e. AI systems with specific transparency obligations: When using AI systems such as chatbots, users should be aware that they are interacting with a machine so they can take an informed decision to continue or step back.

**Minimal risk:** The legal proposal allows the free use of applications such as AI-enabled video games or spam filters. The vast majority of AI systems fall into this category. The draft Regulation does not intervene here, as these AI systems represent only minimal or no risk for citizens' rights or safety.

In terms of governance, the Commission proposes that national competent market surveillance authorities supervise the new rules, while the creation of a **European Artificial Intelligence Board** will facilitate their implementation, as well as drive the development of standards for AI. Additionally, voluntary codes of conduct are proposed for non-high-risk AI, as well as regulatory sandboxes to facilitate responsible innovation.