Strictly regulate high-risk uses of biometrics in AI systems

Why should some uses of biometric data be prohibited in the AI Act but not others?

Under the General Data Protection Regulation (GDPR) and its police counterpart, the Data Protection Law Enforcement Directive (LED), **biometric data are recognised as always sensitive. Our biometric data are permanently linked to our identities, have the potential to eradicate our anonymity, and if they get hacked, can never be re-set**.

When it comes to **remote biometric identification (RBI) in publicly accessible spaces; biometric categorisation on the basis of protected characteristics or when conducted in publicly accessible spaces;** and **emotion recognition** (subject to a strictly-limited potential exemption for assistive purposes), these practices infringe on people's fundamental rights to such an extent that no safeguards can make their use acceptable in a democratic, rule-of-law-respecting society.

Even use cases that do not fall into the above criteria for prohibition can still be unacceptably harmful. Given the sensitivity of biometric data, it is vital that the AI Act supports and builds upon the rights-based frameworks of the GDPR and LED to make sure that data about people's faces and bodies cannot be used against them, and that stronger safeguards are put in place for their use, in order to address the limitations of the risk-based framework of the AI Act. Notably, the need for additional protections of biometric data is foreseen in GDPR Article 9, paragraph 4.

Non-prohibited use cases must still fully comply with existing EU and national rules on data protection (e.g. GDPR, LED), the Charter of Fundamental Rights of the EU, non-discrimination acquis and other relevant laws. **Use cases that are not proven to meet these strict requirements risk disproportionately infringing on people's fundamental rights, and therefore must also be prevented**. More national action is needed to support the enforcement of these rights, and the AI Act's 'high-risk' approach must not be used to enable the uptake of biometric systems that are incompatible with people's rights and freedoms under the GDPR and LED. The approach in this document therefore also relies on additional requirements outlined in our other joint civil society recommendations, for example mandatory fundamental rights impact assessments for all high-risk AI systems.

It is also crucial to remember that **the Act does not provide a legal basis for the processing of personal data in the context of RBI** and, as the European Data Protection Board (EDPS) and

This paper was co-drafted by **European Digital Rights (EDRi)**, **Access Now**, **ARTICLE19**, **Bits of Freedom**, the **Chaos Computer Club (CCC)**, **Digitale Gesellschaft CH** and the **IT-Political Association of Denmark (IT-Pol)**.
It is supported by **AlgorithmWatch**, the **European Center for Not-For-Profit Law (ECNL)**, the **European Disability Forum (EDF)**, **Fair Trials** and the **Panoptykon Foundation**. It follows the Joint Civil Society Statement 'An EU Artificial Intelligence Act for Fundamental Rights', November 2021, signed by 123 organisations.

Supervisor (EDPS) emphasise, the absence of a prohibition does not mean that an AI system is automatically lawful or acceptable.

Recommendations

Recital 23: lex specialis and remote biometric identification (RBI)

Recital 23 clarifies that "this Regulation is not intended to provide the legal basis for the processing of personal data". The recital should be expanded to explicitly emphasise that the *lex specialis* nature of the prohibition on RBI does not provide a legal basis for law enforcement uses of RBI, nor does it weaken existing protections of biometric data under the Data Protection Law Enforcement Directive (LED) or national implementations of the LED.

Article 43(1): enhanced conformity assessments

Given the proven risks to the rights and freedoms of data subjects during the processing of their physical, physiological and behavioural data, and to ensure consistency with the in-principle prohibition of the processing of biometric data under the GDPR and its strict limitation under the LED, extra measures must be taken to prevent the misuse of this highly sensitive data in the cases where such a use is not outright prohibited under the AI Act.

The conformity assessment procedure in article 43(1) should therefore be amended to require third-party conformity assessments for *any* AI system which uses physical, physiological or behavioural data, including biometric data, as the already-established (in the GDPR and LED) high risk of the use of these data - in any context - justifies such additional safeguards.

These conditions should further be elaborated by new articles which would request guidance from the European Data Protection Board (EDPB) on the following criteria within 6 months of the adoption of the AI Act (or, if rules for restrictive measures can be agreed by the co-legislators, potentially via an implementing act):

- Guidance for providers and users, based in and building upon the GDPR and LED, on how to assess the legality, necessity and proportionality of the use of physical, physiological or behavioural data, including biometric data;
- Guidance on the need for law enforcement agencies to have objective, concrete, specific and significant indications that a person is involved in a serious enough crime to justify their singling out for the purpose of the processing of their biometric data; as well as auditable documentation of these reasons, with the possibility for retrospective review and/or appeal; and the removal of the data in the event that (a) no charge is brought within 2 weeks; (b) the person is not convicted after charge; or (c) that there is no match. Equivalent guidance should also be provided for the storage of images / templates in a

This paper was co-drafted by **European Digital Rights (EDRi)**, **Access Now**, **ARTICLE19**, **Bits of Freedom**, the **Chaos Computer Club (CCC)**, **Digitale Gesellschaft CH** and the **IT-Political Association of Denmark (IT-Pol)**.
It is supported by **AlgorithmWatch**, the **European Center for Not-For-Profit Law (ECNL)**, the **European Disability Forum (EDF)**, **Fair Trials** and the **Panoptykon Foundation**. It follows the Joint Civil Society Statement 'An EU Artificial Intelligence Act for Fundamental Rights', November 2021, signed by 123 organisations.

biometric database or repository, which must have a clear legal basis related to specific, serious crimes; must be compliant with the Charter of Fundamental Rights of the EU and the GDPR or LED; have conditions for removal of images or templates; and have measures for redress;

- Self-assessments for providers and users to be checked by the notified body to ensure that the system does not contribute to a normalisation of the use of physical, physiological or behavioural data, including biometric data; and
- Periodic external audits.

Annex III: safeguarding all risky uses of biometrics

To ensure a future-proof approach to the use of biometric systems; consistency with the enhanced protections for sensitive data like biometric data under the GDPR and LED; and to make sure that the use of biometric systems in sensitive domains (e.g. emergency medicine) have high levels of scrutiny and protection given the severe harms when they go wrong, it is essential that heading 1 ("area 1") in Annex III is amended so that any new biometric system that poses a significant risk to fundamental rights can in future be added as a high risk use case.

Finally, to comprehensively protect people's rights and freedoms from abuses of their biometric or biometrics-based data, the specific high-risk use cases under heading 1 ("area 1") should be broadened to include all currently-known risky uses (other than those that we recommend are prohibited).

See the related civil society issue paper on migration and the AI Act for additional high-risk use cases that should be added, as well as the issue papers on biometric categorisation and emotion recognition, to ensure the full protection of fundamental rights.

For more information on these recommendations, please contact ella.jakubowska@edri.org and daniel.leufer@accessnow.org.

This paper was co-drafted by **European Digital Rights (EDRi)**, **Access Now**, **ARTICLE19**, **Bits of Freedom**, the **Chaos Computer Club (CCC)**, **Digitale Gesellschaft CH** and the **IT-Political Association of Denmark (IT-Pol)**.
It is supported by **AlgorithmWatch**, the **European Center for Not-For-Profit Law (ECNL)**, the **European Disability Forum (EDF)**, **Fair Trials** and the **Panoptykon Foundation**. It follows the Joint Civil Society Statement 'An EU Artificial Intelligence Act for Fundamental Rights', November 2021, signed by 123 organisations.