CIVIL LIBERTIES UNION FOR EUROPE

Berlin, 18 July 2025

Liberties' Submission to the Targeted Stakeholder Consultation on Classification of AI Systems as High-Risk

Liberties welcomes the opportunity to contribute to the Commission's Targeted stakeholder consultation on classification of AI systems as high-risk. As a civil society organisation committed to ensuring that artificial intelligence systems fully comply with fundamental rights, we believe these guidelines must clarify existing ambiguities, for example by affirming that the high-risk classification does not undermine the prohibition of RBI systems, emotion recognition technologies, and biometric categorisation tools as set forth in Article 5.

Below are the questions presented in the consultation that we chose to respond to, followed by the full answers we sent to the Commission.

Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems related to biometrics.

The retrospective application of biometric identification analytics to a still image of a suspect taken from CCTV footage of a serious crime, where the footage is obtained lawfully (i.e post RBI). By definition, any real-time RBI system by police that is not prohibited would still be high risk, and would also have to follow the additional controls required for police uses of RBI. We reiterate that these use cases still entail extremely severe limitations on the fundamental rights of all people in the public spaces. The exceptions to the in-principle prohibition therefore need to meet an extremely high threshold. In a situation such as an imminent, genuine and foreseeable threat of a terror attack, there must still not be any permanent RBI infrastructure. Instead, the infrastructure must be temporary, clearly marked, and must meet all the criteria for authorisation, safeguards, limitations in geographic scope etc in order to meet requirements of strict necessity and proportionality. Any uses not meeting these strict criteria would still be prohibited.

Do you have or know practical examples of AI systems related to biometrics where you need further clarification regarding the distinction from prohibited AI systems?

The Hungarian FRT Act introduces a broad legal basis for the use of remote biometric identification (RBI) without specifying any technical or procedural safeguards for police operations. This effectively permits a system of remote biometric identification that is prohibited under Article 5(1)(h) of the EU Artificial Intelligence Act (AI Act). Article 5(1)(h) of the AI Act bans the use of real-time RBI systems in publicly accessible spaces for law enforcement purposes, unless certain strict exceptions apply and such use is authorised under national law with appropriate safeguards. Although courts have not yet interpreted the AI Act, there are compelling reasons to conclude that Hungary's FRT law violates Article 5(1)(h). Assuming it is undisputed that the system constitutes RBI in public spaces, two central questions must be addressed. Under Article 3(42) of the AI Act, a real- time RBI system is defined as one in which biometric data is captured, compared, and matched without significant delay, including cases with "limited short delays." Recital 17 confirms this includes "near-live" material, while the AI Act Prohibition Guidelines (para. 310) clarify that a use is real-time unless the delay is so significant that the individual has likely already left the scene. Section 12/A of Hungary's FRT Act enables real-time identification by linking newly recorded material to the HIFS database, allowing police to identify individuals, such as protesters, within moments. This clearly falls under the definition of real- time RBI and is therefore covered by Article 5(1)(h). Additionally, the Hungarian law undermines the purpose of the AI Act prohibition, as stated in Recital 32, which highlights the chilling effect of such surveillance on public participation and freedom of assembly. A system that allows authorities to identify people at demonstrations in real time significantly deters individuals from exercising their fundamental rights. For more, see: https://www.liberties.eu/f/tcbfhu

If you see the need for clarification of the high-risk classification in Point 1 of Annex III to the AI Act and its interplay with other Union or national legislation, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay

The guidelines must affirm that the high-risk classification does not undermine the prohibition of RBI systems, emotion recognition technologies, and biometric categorisation tools as set forth in Article 5. This clarification is essential to uphold the rights enshrined in the Charter of the European Union. EU data protection authorities have consistently underscored that facial recognition in law enforcement contexts must fully comply with the LED. This includes the need for a clear and explicit legal basis, a demonstration of necessity and proportionality, strict data minimisation, independent oversight, and prior completion of DPIAs. The guidelines must emphasise that any deployment of biometric AI by public authorities must remain strictly exceptional and meet the high threshold established by EU law, particularly respecting Charter Articles 7 and 8. This requires the guidelines to explicitly articulate how Article 5 exceptions under the AI Act align with broader legal obligations—including the need for judicial authorisation and democratic oversight under national laws implementing EU frameworks on police cooperation. The guidelines must clarify that non-remote BI systems are inherently high-risk and must be regulated in line with Article 9 of the GDPR. RBI used for non-law enforcement purposes are prohibited under Article 5, and that any system capable of operating in real-time or near real-time must all within the scope of full ban.

If you see the need for clarification of the high-risk classification in Point 8 of Annex III to the AI Act and its interplay with other Union or national legislation, in particular Regulation (EU) 2024/900 on targeted political advertising, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay

It is unclear whether AI systems used for targeting, personalization, or behavioral prediction in political ads are automatically deemed high-risk under the AI Act or only when intended to influence voting—raising questions around how "intent" and "impact" are assessed. Article 6 of the Political Ads Regulation introduces safeguards for targeting and amplification, but many such systems rely on algorithmic profiling, potentially triggering obligations under the AI Act. It is unclear whether compliance with Article 6 fulfills AI Act duties or if additional assessments, including FRIAs are required. AI-based microtargeting often involves inferred sensitive data (e.g. political views, ethnicity), raising further legal questions. GDPR prohibits processing of such data without valid exceptions, and divergent treatment under the Political Ads Regulation and AI Act complicates compliance. The lack of clarity risks enabling voter manipulation systems to evade oversight. Dual but unaligned regulations may confuse deployers and hinder enforcement. Authorities may also clash over jurisdiction.

Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems listed in Article 26 for which you would seek clarification, for example through guidelines? If so, please elaborate on which specific questions you would seek further clarification.

Regarding the use of post-remote biometric identification (RBI) under Article 26, the guidelines must clearly define the specific and limited conditions under which authorisation may be granted. To qualify as permitted (but still highly restricted) post-RBI, such systems should be limited strictly to the analysis of still images—such as screen grabs—of individual faces belonging only to persons suspected of serious crimes. It must be ensured that no biometric data or features of non-suspect individuals are processed. A comprehensive analysis of the entire footage would constitute untargeted biometric surveillance, which is explicitly prohibited under Article 26. Furthermore, even where a specific use case is not formally prohibited under the AI Act, it may still contravene the EU Charter of Fundamental Rights, particularly if the system demonstrates discriminatory performance across demographic groups—for instance, reduced accuracy for people of colour—or is disproportionately applied to those communities. In line with the Law Enforcement Directive, no decision with legal effect may be based solely on output from these systems. Exceptions to the general prohibition must meet an exceptionally high threshold. For example, even in scenarios involving imminent, genuine, and foreseeable terrorist threats, RBI infrastructure must be strictly temporary, clearly marked, and subject to rigorous safeguards—including limitations on geographic scope and purpose—to ensure absolute necessity and proportionality. Use cases that fail to meet these criteria remain prohibited. The guidelines must also clarify that the authorisation mechanism in Article 26 does not legitimise the problematic practices referenced in Question 8, which, in fact, amount to

prohibited uses under Article 5 and Recital 17. Specifically: In Hungary, recent legislative amendments authorise the use of RBI in publicly accessible spaces by law enforcement. Although the government claims compliance with the AI Act due to the system's 'near-instant' nature, the guidelines must state unequivocally that this type of deployment constitutes a prohibited practice, as defined in Article 5 and Recital 17.

Are there aspects related to the obligations for deployers of high-risk AI systems listed in Article 26 which require clarification regarding their interplay with other Union legislation? If so, please elaborate which specific aspects require clarification regarding their interplay with other Union legislation and point to concrete provisions of specific other Union law.

Transparency must be central to the FRIA process: findings, including the impact assessment itself and decisions must be publicly accessible to affected individuals, civil society, and oversight bodies. The FRIA process should be open to feedback and scrutiny. The Guidelines should advise on pre-existing systems because the exemption undermines both fundamental rights protection and single market cohesion. -Practical implementation requires robust templates that go beyond checklists and offer procedural clarity. Templates must include open-ended sections to capture context, deliberation, and system-specific nuances. -Stakeholder participation is vital. Deployers must document efforts to include affected groups, civil society, and experts. This includes acknowledging missing perspectives, power imbalances, and resource allocation. Article 77 bodies should be involved in risk mitigation where appropriate. - FRIAs should not only identify risks but justify the deployment itself, assessing necessity and proportionality. They must include clear mitigation and redress plans, published and accessible. - Although Article 27(2) allows reuse of provider-conducted FRIAs, deployers must still carry out context-specific assessments, explaining how provider analysis was adapted and what risks emerged in their unique environment. -The transparency framework must specify what information is public, and under what conditions redactions are permissible. Justifications for withholding data must be provided. Competent authorities, including Art. 77 bodies, must have full access, and individuals must be informed of their rights and redress mechanisms. - To ensure accountability, FRIA templates should include sections on external reviews, complaint procedures, and interactions with market surveillance or oversight authorities. The template should prompt deployers to: define measures for ongoing monitoring of rights impacts post-deployment, describe mechanisms for affected individuals to challenge decisions or request human review and outline plans for revising or halting deployment if unacceptable risks emerge.

Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems for the fundamental rights impact assessment for which you would seek clarification in the template?

FRIA template must compel deployers to move beyond superficial or compliance-driven approaches and undertake meaningful, evidence-based, and participatory evaluations of AI's

potential impact on fundamental rights. Without such rigor, Article 27 risks losing its protective power and becoming symbolic rather than enforceable. We urge the AI Office to adopt a fully transparent and consultative process in finalizing the template—one that actively includes civil society organizations, whose expertise and insights are essential to safeguarding rights in practice.

In your view, how can complementarity of the fundamental rights impact assessment and the data protection impact assessment be ensured, while avoiding overlaps?

The guidance must clearly articulate the differing focus and function of Fundamental Rights Impact Assessments (FRIAs) and Data Protection Impact Assessments (DPIAs). While DPIAs primarily address privacy-related concerns—such as data minimisation, lawfulness of processing, and discrimination linked to personal data—FRIAs serve a broader purpose. They assess potential impacts on the full spectrum of fundamental rights, including human dignity, equality, social protection, freedom of expression, and access to essential services. High-risk AI systems often pose threats to fundamental rights that extend beyond data protection. Although FRIAs can be informed by DPIA findings, the two processes are not interchangeable, and a DPIA alone does not satisfy the AI Act's expectations for robust rights assessments. Promoting Synergy Between DPIA and FRIA Processes Engagement should go beyond data subjects to involve affected or vulnerable communities, and the mitigation strategies must be tailored to both privacy and broader rights risks. From a documentation standpoint, it is more effective and transparent to maintain separate records for DPIAs and FRIAs. This approach ensures legal certainty for deployers across jurisdictions where DPIA frameworks are already in place and avoids resistance to abandoning custom-built tools. Moreover, given current ambiguity around whether Data Protection Authorities (DPAs) will oversee FRIAs, distinct documentation provides clarity for future regulatory enforcement under the AI Act. Furthermore, structured information exchange between AI providers and deployers is essential to ensure that both DPIAs and FRIAs are grounded in system design as well as real-world deployment contexts.

Do you have any feedback on issues that need clarification as well as practical examples on the application of the concept of 'substantial modification' to a high-risk AI system.

The Guidelines should establish clear thresholds and detailed criteria for what constitutes "substantial modification", specifying exactly which types of modification require new conformity assessment. This is essential to ensure that AI systems do not evolve without proper oversight, potentially exposing people to harm without adequate protection or accountability. The Guidelines must explicitly define any modification that leads to the reclassification of an AI system as high-risk as a "substantial modification." Apart from being integrated in GPAI systems, LLM models or other algorithmic systems can also be integrated in high-risk AI systems. Given the rapid pace of advancement in large language models (LLMs) and other algorithmic systems , it is expected that companies will regularly replace or upgrade the

underlying models in their AI systems to take advantage of improved or different performance and reasoning capabilities. Guidelines should explicitly state that any upgrade or change to an AI system involving the integration of a new or changed LLM is considered a substantial modification under the AI Act, even more crucially so, when LLM plays a crucial role in decision-making.

Do you have or know concrete examples of AI systems that in your opinion need ***to be added to the list of use cases in Annex III, among the existing 8 areas, in the light of the criteria and the conditions in Article 7(1) and (2)*** *and should be integrated into the assessment pursuant to Article 112(1) AI Act? If so, please specify the concrete AI system that fulfils those criteria as well as evidence and justify why you consider that this system should be classified as high-risk.*

Non-remote uses of biometric identification systems must be added in Annex III. Biometric identification is not the same as verification (sometimes known as 1:1 matching), which includes things like unlocking your phone or using a passport with a biometric chip to go through the ePassport gate at an airport. Biometric identification is a process of comparing one's data to multiple other sets of data (1:many) in some form of database. Non remote uses of biometric identification carry dangerous risks of discrimination, unlawful and disproportionate surveillance as well as data leaks. Considering Articles 7 (2) (e) and (h), biometrics identification systems by law enforcement authorities are already proven to increase racial profiling practices and discriminatory stop- and-search practices, as ethnicity or skin colour is viewed as a proxy for an individual's migration status or a link to criminal behaviour proved to discriminate against [https://racialjusticenetwork.co.uk/reports/7027/]. Considering Article 7 (2) (b) the likelihood for these systems to be used by police and migration authorities is extremely high as biometric identification has been indicated as priority in the framework of EU home affairs and migration policies.

Contact: Civil Liberties Union for Europe
Eva Simon
Email: eva.simon@liberties.eu
Website: liberties.eu
Address: c/o Publix
Hermannstraße 90 12051 Berlin/ Germany