July 18th 2025

Contribution to "targeted stakeholder consultation on classification of AI systems as high-risk"

Authors (alphabetical order): Alessandra Calvi[*†], Simone Casiraghi, Pia Groenewolt[*], Cesar Augusto Fontanillo Lopez[*‡], Maciej Otmianowski[*], Federica Paolucci[§], Niels van Dijk[*]

As researchers affiliated with the d.pia.lab, a network of legal and philosophical scholars focused on data protection, AI regulation, and risk and impact assessments, we welcome the opportunity to contribute to the European Commission's public consultation titled *Targeted stakeholder consultation on classification of AI systems as high-risk* ([link]). This document reproduces the input submitted via the official template provided by the Commission and is structured accordingly.

About the d.pia.lab

The Brussels Laboratory for Data Protection & Privacy Impact Assessments, or d.pia.lab, connects fundamental, methodological and applied research, provides training and delivers policy advice related to impact assessments in the areas of innovation and technology development. Whilst legal aspects of privacy and personal data protection constitute its core focus, the Laboratory includes other disciplines, including ethics, philosophy, surveillance studies and science, technology & society (STS) studies. Established in November 2015, the Laboratory constitutes a part of and builds upon the experience of the Research Group on Law, Science, Technology & Society (LSTS) at the Vrije Universiteit Brussel (VUB), Belgium.

This document shares the input we submitted through the official template provided by the Commission. It is structured in accordance with the format and guidance set out in the consultation framework. As we were not constrained by character limits, it does go beyond the submitted text using fewer acronyms to ease reading. The format offered here shares the questions from the consultation (in orange) and the response to offer a structure.

[*] Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab), Research Group on Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel (VUB)
[†] CY Cergy Paris Université, ENSEA, CNRS | ETIS UMR 8051
[‡] Centre for IT & IP Law (CiTiP), KU Leuven
[§] Baffi Centre, Bocconi University

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.

P=premise and C=conclusion

- P1: Point 1 of Annex III AIA lists high-risk AI systems in the area of biometrics by referencing 'remote biometric identification systems', 'biometric categorisation', and 'emotion recognition'.
- P2: The definitions of 'remote biometric identification systems' (Art. 3(41) AIA), 'biometric categorisation' (Art. 3(40) AIA), 'emotion recognition' (Art. 3(39) AIA), and 'biometric verification' (Art. 3(36) AIA) are built on the concept of 'biometric data' (Art. 3(34) AIA).
- P3: Biometric data (Art. 3(34) AIA) is not construed on the basis of a unique identification interest, while biometric data (Art. 4(14) GDPR; Art. 3(13) LED; Art. 3(18) EUDPR) is construed on the basis of a unique identification interest.
- P4: The AIA is enacted on the basis of Art. 114 TFEU, and when the AIA contains specific rules on 'remote biometric identification', 'risk assessments' and 'biometric categorisation' for the purpose of law enforcement, the AIA is enacted on the basis of Article 16 TFEU; the GDPR, LED, and EUDPR are all enacted on the basis of Article 16 TFEU.
- P5: Biometric identification and biometric authentication are both considered sensitive personal data processing under GDPR (Rec. 51) and EUDPR (Rec. 29), while Point 1 of Annex III AIA lists excludes it from the list of high-risk AI systems.

C1: Is it sound to interpret that, where biometric data processing does not concern law enforcement purposes, two conflicting definitions of biometric data coexist under different instruments of EU law?

C2: If so, how should the compatibility or incompatibility of those two definitions of biometric data enacted on different EU legal bases be interpreted?

C3: Is the different treatment of biometric authentication in the AIA and the data protection framework leading to inconsistent levels of protection across EU laws?

C4: To the extent that the AIA and the LED stem from Art. 16 TFEU but provide different definitions of biometric data, is there a legal antinomy between definitions when such biometric data is processed for biometric identification and categorisation for law enforcement purposes?

C5: If so, shall the definition of biometric data under the AIA act as lex specialis to the LED to solve this conflict?

- P1: Point 1 of Annex III AIA lists biometric categorisation as a high-risk AI system i.r.w. Article 6(2) AIA, while Article 6(2) AIA creates an additional rule to Art. 6(1) AIA, and while Article 6(1) AIA refers to high-risk systems irrespective of whether they are placed on the market or put into service.
- P2: Article 5(g) AIA lists biometric categorisation as a prohibited practice.

C1: Does Art. 6(2) AIA refer to AI systems for biometric categorisation as high risk, irrespective of whether they are placed on the market or put into service, while Article 5(g) AIA refers to biometric categorisation provided they are placed on the market or put into service?

C2: Making a joint reading of both provisions, does the AIA implement a 'phasing' criterion whereby the more advanced the biometric categorisation system is in its life cycle, the harsher the legal response is, provided the constraints of Art. 5(g) AIA are met?

C3: Are AI-based biometric categorisation system considered high risk 'in themselves', according to 6(2) AIA i.r.w. Point 1 Annex III AIA, and are AI-based biometric categorisation systems considered a prohibited practice according to Article 5(g) AIA only when placed on the market, put into service, or used, safe exceptions?

Beyond the technical standards under preparation by the European Standardisation Organisations, are there further aspects related to the AI Act's requirements for high-risk AI systems in Articles 9-15 for which you would seek clarification, for example through guidelines? If so, please elaborate on which specific questions you would seek further clarification.

Risks to fundamental rights – The existence of a risk to fundamental rights is a condition for the application of Art. 9, but this notion remains unclear. The guidelines need to provide examples of risks to rights. The guidelines should provide a more detailed methodology to assess the level of interference with those rights. Should rights from the EU secondary law be considered? For example, the consumer's right to withdrawal (Art. 9, Directive 2011/83/EU), which is not directly in the European Charter of Fundamental Rights, however, it contributes to the high level of consumer protection mentioned in the Art. 38 of the Charter.

We claim that the application of **the proportionality principle** in resolving conflicts between non-absolute fundamental rights requires further clarification (Art. 52(1) of the Charter). The ECHR and the case law of the European Court of

Human Rights (ECtHR), along with the fundamental rights and constitutional traditions of the Member States, should serve as key interpretative and substantive references for deployers when conducting the FRIA.

Risks to be mitigated under Art. 9 – Inconsistencies between Art. 9 and Rec. 65 raise uncertainties as to which risks are to be mitigated. Under Art. 9(2)(a)(d), risk management measures concern only the known and reasonably foreseeable risks when a system is used according to its intended purposes. Other risks (e.g., emerging from foreseeable misuse or the post-market monitoring system) are evaluated but not managed. Yet, under Rec. 65 AIA, the provider implements mitigation measures for the known and reasonably foreseeable risks of AI systems considering their intended purpose and reasonably foreseeable misuse.

Interplays 'known and reasonably foreseeable' risks and risks emerging from post-market monitoring – Thanks to post-market monitoring, knowledge about risks evolves. Clarification is needed to evaluate under what conditions risks emerging from post-market monitoring become 'known and reasonably foreseeable'. Moreover, we would welcome the criteria that could help distinguishing the "known and reasonably foreseeable" risk from those which are not.

Publicity and understandability of technical documentation – Typical addressees of technical documentation are deployers, downstream providers, and regulatory authorities checking compliance. But its availability to e.g., non-tech experts, NGOs, and research institutions would facilitate external scrutiny of AI systems. Meanwhile, design choices of providers may affect fundamental rights. Thus, clarification as to the publicity and understandability of technical documentation by not solely a technical audience is desirable. Furthermore, clarification is needed on how to account for the cumulative impact of multiple AI systems or processing operations in a single organisation, e.g., how the deployment of multiple systems may interact and exacerbate risks to rights, such as compounding bias or limiting access to remedies.

Question 36. ***(limit: 3000 characters)***
Are there aspects related to the requirements for high-risk AI systems in Articles 9-15 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.

Relation between cybersecurity requirements. Cybersecurity risk assessment Art. 15(5) AIA and NIS2. What is the relation between those requirements? What

is the relation between the status of as a "essential" or "important" entities (Art. 3 NIS2) and AI system provider in the cybersecurity risk assessment responsibilities? The cybersecurity requirement is rather not detailed in the AI Act, so it is important to understand how it relates to existing cybersecurity requirements. For example, who and how should conduct cybersecurity risk assessment in the context of AI systems applied in essential or important entities (NIS2) and how those assessments relate to each other.

Are there aspects related to the obligations for providers of high-risk AI systems 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.

The interplay between:

1) the risk management system (art 9) and possibly the risk assessment (art 55) for GPAI models with systemic risk] in the AI Act,
2) the systemic risk assessment in the Digital Services Act (art 34, esp. 34(1)(b)) and GPIA model systemic risk assessment (Art. 55 AI Act),
3) the data protection impact assessment under the GDPR (Art 35) and fundamental rights impact assessments deserve further clarification.

Clarification is needed as to whether one consolidated risk assessment could be structured in layered or modular form, especially for providers of GPAI systems embedded in VLOPs. Common guidance should support interoperable templates and harmonised terminology across these frameworks.

As a matter of fact, these tools have possibly many overlaps in terms of scope (data processing activities and GPAI AI models are both crucial for VLOPs and VLOSEs for providing digital services) and types of risks assessed in relation to fundamental rights, especially regarding privacy and misinformation. As for the GDPR, the same entities conducting risk assessments under the DSA are likely subject to the obligation to conduct a (DPIA) under Article 35 of the GDPR, including "an assessment of the risks to the rights and freedoms of data subjects" that may arise from how controllers process personal data through new technologies, such as algorithmic systems. As for the AIA, AI systems may be embedded in VLOPs and VLOSEs subject to risk-management obligations (Rec. 118 AIA) and the obligations on providers of AI systems are "particularly relevant" for the implementation of the DSA (Rec. 119, 120, 136 AIA), especially concerning the identification and mitigation of systemic risks.

Furthermore, the AI Act introduces obligations for both GPAI model providers (Art. 55) and deployers using GPAI systems but does not clarify how risk assessments should be shared or divided. Similarly, under the DSA and GDPR, different actors

may serve as controllers, processors, or providers. Clarification is needed on how responsibility for risk identification, documentation, and mitigation is to be allocated in multi-actor supply chains, especially in cases involving foundation models integrated into downstream services.

Timeline of the assessments: Additionally, clarification is needed on how reassessment obligations align across instruments. While the AI Act mandates pre- and post-market monitoring and updates to the risk management system, the DSA requires annual systemic risk reassessments for VLOPs. GDPR-based DPIAs must also be updated when the nature, scope, or purposes of processing change significantly. A cross-regime approach should ensure that reassessment timelines and triggers are coordinated to avoid contradictory or outdated assessments.

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.

A clearer interplay between Article 26 AIA and other Union legislation is needed, particularly the GDPR and sector-specific obligations under the Law Enforcement Directive (LED). Clarifications should be provided in two areas:

- **Overlap with GDPR's obligations:**
  Deployers are often also data controllers under the GDPR, and Article 26 obligations, such as ensuring appropriate human oversight and providing transparent information, are closely intertwined with GDPR Articles 5, 12–14 (transparency) and 22 (automated decision-making). However, the AI Act does not specify how deployers should reconcile potential conflicts or duplications in compliance steps. Clear guidelines should clarify to what extent AI Act obligations are cumulative or derivative from existing GDPR obligations.
- **Sector-specific rules:**
  In the case of biometric systems used by law enforcement authorities (e.g., FRT), Article 26 obligations overlap with LED requirements on necessity, proportionality, and data minimisation. Particularly under Article 13 and Article 14 LED, individuals have the right to be informed about the processing of their personal data and may request access, rectification, restriction, or erasure, unless such rights are restricted under Article 15 LED due to compelling operational reasons (e.g. ongoing investigations). Importantly, these rights may be exercised by any individual whose personal data is processed by competent authorities for law enforcement purposes, including suspects, witnesses, and even bystanders, provided that exercising such rights does not jeopardise law enforcement tasks.

In practice, this may include individuals unknowingly captured in biometric surveillance systems (FRT) who might wish to challenge the lawfulness of data processing or automated risk profiling. Clarification is needed as to how the obligations imposed on deployers under Article 26 AI Act (including human oversight and transparency duties) interrelate with the LED rights regime, particularly where individuals face difficulties in accessing meaningful explanations or challenging the deployment of high-risk AI systems due to the LED's lawful limitations. This legal intersection warrants guidance to avoid systemic opacity and preserve the right to effective remedies.

Deployers may lack technical capacity to assess risks independently and often rely on providers' documentation (e.g., interactions between Art. 9 and Art. 27 AI Act). However, Article 26(2) assigns deployers independent responsibilities for ensuring compliance. Guidelines are on: i) whether and how deployers can rely on technical documentation and testing results from providers to meet their legal obligations, especially under the principle of accountability enshrined in the GDPR, ii) and on how deployers coordinate overlapping requirements across the AI Act, GDPR, and LED, with a particular emphasis on shared responsibilities and legal hierarchy in case of normative conflict.

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?

Formulation of the questions in the FRIA questionnaire – The questions should be formulated to prompt critical reflection and explicitly require deployers to analyse the potential implications and harms of the AI system from an intersectional perspective including gender, race, ability, social status, age, and other relevant factors. The template should therefore go beyond a box-ticking exercise and must not be fully automatable.

Granularity of fundamental rights – It is unclear whether using the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union (CFREU) as a benchmark is adequate, considering its limited horizontal effects, and sufficient, due to the lack of elaboration on certain rights (e.g., the CFREU recognises environmental protection as a principle, but does not operationalise it into substantive environmental rights - such as right to a healthy environment - which may conversely be recognised in EU member states).

Complementary guidance could draw from existing structured methodologies such as HUDERIA (Council of Europe), which integrates human rights, democracy, and the rule of law in a single risk matrix. FRIA could benefit from aligning with this

framework or incorporating lessons from HRIA practice (e.g., under the CSDDD proposal), to promote coherence in horizontal application of rights.

Assessing risks to fundamental rights – Combining probability and severity of harm to assess the risks to fundamental rights may be insufficient. In a FRIA, multiple rights may clash and deployers may have to choose which to prioritise. To do so, they may resort to other techniques beyond traditional risk management, typical of the legal domain, such as a necessity and proportionality assessments, for which they need guidance.

Participation in the assessment – In line with Recital 96, the template needs to provide guidance on how to effectively identify and when to involve stakeholders in the FRIA, including the collection of feedback from end-users as to the effectiveness of mitigation measures such as human oversight and complaint mechanisms. Clarification is needed regarding which categories of stakeholders are "relevant" and when a consultation might be "appropriate".

Composition of the team of assessors – The assessment process requires multiple types of expertise. The template needs to provide guidance to ensure diversity in the team of assessors regarding the necessary knowledge and know-how.

Revision of the assessment process and the template itself – An assessment is an iterative process that requires periodic revision. The template should specify the criteria that trigger periodic revisions. The template is also a living document that might require adjustments. A feedback mechanism on the template questionnaire, functional to its periodic revisions, needs to be established.

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

Interdependency of DPIA and FRIA – The FRIA should explicitly state that it builds on the DPIA but extends the scope of risk assessment to include fundamental rights such as freedom of expression, freedom of assembly, and non-discrimination. A layered template could allow deployers to attach a valid DPIA when addressing Art. 8 CFREU and, to some extent, Art. 7 CFREU, while the FRIA should focus also on the residual rights impacts not covered by the GDPR. If a DPIA already exists, a FRIA need not duplicate the assessment on data protection right. Yet, an AI system in compliance with data protection and GDPR may impact other fundamental rights and require adjustments, also considering cumulative effects. The other way around, a FRIA may trigger a DPIA revision.

Exchange of information – Entities performing the DPIA and FRIA may be different and need to exchange information without compromising legitimate secrecy. They

would benefit from the creation of a framework for information exchange. Moreover, harmonising scales of risk likelihood, severity, and mitigation tools can enhance interoperability. Regulatory guidance should encourage the use of compatible risk indicators, and institutional coordination between DPOs and fundamental rights officers should be formalised.

Participatory assessment – Entities performing the DPIA and FRIA may need to consult stakeholders during the process. As there may be an overlap in the categories of stakeholders affected, the same consultation activities (depending on the methods chosen and providing that pertinent questions are asked) could be beneficial for both processes. Additionally, the criteria for assessing "whether it is appropriate" are needed. When and under what conditions those subject to regulation should be required to include stakeholders in the assessment process, and how they may justify their decision not to involve them.

Summaries of FRIA and DPIA which are related to AI systems deployed by public authorities should be published in the EU database (Art. 26(8), 49(2)(3), and 71 AI Act). The scope of information to be included is unclear. We propose the following information to be required: details on the risk assessed, the mitigatory measures, and proportionality assessment justifications (why the specific AI system, processing activity is proportional to the purpose of processing/deployment of the AI system in the light of the assessed risks. Additionally, the date of the original assessment, the last reassessment and next planned revision, and the actors involved in the assessment process. The EU database should also reflect cumulative risks and historical changes, particularly for deployments in sensitive contexts where revisions may be prompted not only by technical updates but by shifts in public expectations, case law, or complaints from affected groups.

Are there aspects related to the AI Act's right to request an explanation in Article 86 for which you would seek clarification, for example through guidelines?

Operationalisation of the right to explanation – Clarification is needed:

- Regarding the preconditions for exercising the right, these include: 1) transparency about the use of an AI system, and 2) information about the existence of the right itself.
- Scope of 'clear and meaningful' explanation, considering that it provides a basis on which the affected persons can exercise their rights (Rec. 171). Depending on the recipient and on the right to be exercised, such an explanation requires adjustments. The notion of a "clear and meaningful" explanation (Art. 86(2)) must be adaptable to the recipient's context, e.g., laypersons vs legal professionals. Drawing on case law and the jurisprudence surrounding Art. 22 GDPR, guidance should distinguish between descriptive (what happened), procedural (how it happened), and normative (why it was legitimate) layers of explanation.

- 'Legal effects or similarly significant' based on case law on Art. 22 GDPR, if appropriate.
- interplays Art. 86 AIA and Art. 22 GDPR. Art. 86's reference to "legal effects or similarly significant" consequences mirrors GDPR Article 22, yet its independent legal basis could create parallel obligations. Clarification is needed on whether individuals can exercise both rights concurrently and how supervisory authorities should coordinate enforcement.

Do you have or know concrete examples of AI practices that in your opinion contradict Union values of respect for human dignity, freedom, equality and no discrimination, democracy and the rule of law and fundamental rights enshrined in the Charter and for which there is a regulatory gap because they are not addressed by other Union legislation? If so, please specify the concrete AI system that fulfils those criteria and justify why you consider that this system should be prohibited and why other Union legislation does not address this problem.

Use of AI in border management - Several scholars (among others: Molnar, Mahmoudi, Vavoula) and NGOs have criticised certain uses of AI systems for border management as highly oppressive, discriminatory, based on gender and racialised assumptions, and sometimes on pseudoscience (e.g., lie detectors). Despite that, EU legislators choose not to ban them, but to reconduct them to high-risk AI systems or introduce exceptions. EU legislators need to re-consider their choices.

AI is increasingly used to support overstretched administrative systems where human capacity is limited. However, when these decisions affect fundamental rights, like the right to reside or access education, efficiency must not override legal safeguards such as the right to good administration (Art. 41 of the EU Charter).

Despite this, the AIA allows such systems especially in migration and public service delivery to operate as "high-risk" rather than prohibiting them. While this classification brings obligations (e.g., transparency, human oversight), it still permits deployment in sensitive areas where structural risks of error or bias are high. Legislators should consider whether, in such contexts, tighter restrictions or outright bans are warranted.

AI systems processing non-personal data like food safety alerts or environmental metrics typically fall outside the scope of data protection laws such as the GDPR. This gap can have serious consequences. In Canada, an AI system monitoring food safety failed to flag an outbreak due to lack of oversight, causing a delayed response that led to hospitalisations and deaths.

While the AIA treats health-related systems as high-risk, it doesn't extend core data protection safeguards like accuracy, purpose limitation, or the right to contest decisions to systems using non-personal data. Nor does it mandate sufficient sectoral oversight beyond what exists in EU food and environmental law, which may not reflect AI-specific risks. This suggests a need to extend GDPR-like

safeguards especially accuracy, oversight, and contestability to AI handling sensitive non-personal data.

In Finland, the migration authority introduced automated decision-making for permanent residency applications. While designed to reduce backlogs, the system risks issuing unjust decisions, especially amid rising anti-immigrant sentiment and legal tightening. Civil society including groups I work with opposed this during consultation, yet the programme moved forward regardless.

This is not a clear regulatory gap under the AIA, which permits such systems under high-risk rules. But it raises a broader concern: what happens when public consultation is ignored? The AIA only requires stakeholder consultation in limited contexts and offers no real remedy when democratic input is sidelined. Stronger accountability such as binding public participation or impact assessment mechanisms should be embedded into the AIA for high-risk public systems.