Introduce obligations on users of high-risk AI systems

This document outlines amendments to introduce obligations on users of high-risk AI. In particular, these recommendations are designed to facilitate greater transparency as to how high-risk AI is used, and ensure accountability and redress for uses of AI that pose a potential risk to fundamental rights.

How does the AIA regulate 'users' of high-risk AI?

The Artificial Intelligence Act (AIA) predominantly imposes requirements on 'providers' (developers) rather than on the 'users' (deployers) of high-risk AI. For the majority of high-risk AI uses in Annex III, compliance with the regulation's requirements (articles 8-15) is self-assessed by the providers themselves, pursuant to article 43(2).

The AIA imposes minimal obligations on users of high-risk AI systems. Article 29 outlines the duties of users of high-risk AI: to use the system in conjunction with the providers' 'instructions of use', ensuring relevant data, and monitoring of the system. However, the user is not obligated to undertake any further measures to analyse the potential impact on fundamental rights, equality, accessibility, public interest or the environment, to consult with affected groups, nor take active steps to mitigate potential harms.

Why the AIA needs obligations on users

The following outlines why the AIA needs obligations on users of high-risk AI:

- **Foresight of AI harms in the context of use as well as design**

A crucial flaw of the current AIA approach is that it overlooks the complexity of AI systems and the importance of the **context** within which they are used to be able to assess impact on fundamental rights, people and society. This is particularly true for 'standalone' AI systems defined under article 6(2), which display a wide and more complex range of risks than for products. As such, legislative approaches geared toward product safety will not be sufficient to address these broader implications for fundamental rights.[1] Whilst the provider-led conformity assessment process may identify the core technical shortcomings of the system, this process is fundamentally ill-suited to identify the risks in the context of deployment.

For example, a facial authentication system may meet the technical requirements specified in the Act yet still pose significant fundamental rights violations, compromise data protection and non-discrimination law, and disproportionate surveillance in the context of deployment (i.e. in a specific shopping centre) creating chilling effects on the enjoyment of fundamental rights.

Further, the requirements on providers in the AIA are highly technical in nature, and are thus insufficient as a mechanism to prevent or mitigate risks to fundamental rights, structural harms, or economic or environmental shifts engendered by the introduction of AI systems in certain contexts.[2] Such considerations are inherently better assessed by the users in light of the context of deployment of the AI system.

---

1 Oxford Commission on AI & Good Governance (2021). Harmonising Artificial Intelligence: the role of standards in the EU AI Regulation. Available: https://oxcaigg.oii.ox.ac.uk/wp-content/uploads/sites/124/2021/12/Harmonising-AI-OXIL.pdf

2 For further information as to the limits of technical mechanisms to prevent AI harms, see EDRi (2021). *Beyond De-biasing: Regulating AI and its inequalities:* https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf, authored by Dr Seda Gürses and Agathe Balayn of Technical University Delft.

This paper was drafted by and with the support of European Digital Rights (EDRi), Access Now, Algorithm Watch, Bits of Freedom, European Disability Forum (EDF), European Not for Profit Law Center, Fair Trials, Panoptykon Foundation, and PICUM. It follows the Joint Civil Society Statement 'An EU Artificial Intelligence Act for Fundamental Rights' signed by 123 organisations in November 2021.

- **Facilitating accountability of users of high-risk AI**

While some of the risk posed by the systems listed in Annex III come from how they are designed, significant risks stem from how, and the purpose for which, they are used. This means that providers cannot comprehensively assess the full contextual impact of a high-risk AI system during the conformity assessment, and therefore that users of high-risk AI must be assigned obligations in the AIA to uphold fundamental rights in addition.

Member States have already demonstrated willingness to implement governance obligations on users of AI systems. For example, in the Netherlands the Ministry of Interior and Kingdom Relations has developed the Impact Assessment Mensenrechten en Algoritmes (IAMA) that requires public authorities to conduct impact assessments.[3] Speaking in Brussels in March 2022,[4] Dutch Minister for Digitalisation Alexandra van Huffelen questioned:

> *"The AI act asks developers to assess certain risks and privacy legislation asks deployers to assess privacy risks in particular. But is this enough? In the Netherlands we have already developed a broader Impact Assessment tool on Human Rights and algorithms. It asks all parties involved in the entire product cycle of an AI system to consider fundamental rights risks."*

The obligations outlined in the following amendments would require users to delineate the impacts of high-risk AI systems, publish the findings and therefore create a crucial tool of accountability over how high-risk AI systems are deployed. As stated below, the obligation to (a) conduct and publish a fundamental rights impact assessment and (b) register uses of high-risk AI systems will create the necessary mechanism of public transparency by which people affected by high risk AI, and public interest organisations, are able to access the information to oversee, and if necessary, challenge these systems when they infringe on fundamental rights. One of the goals of the AIA is to foster an ecosystem of trust and excellence, and having users of high-risk AI systems assess the impact of their deployments and be transparent about the systems they are using will be key to building public trust in this technology.

- **Countering dominance of AI providers**

Obligations on users of high risk AI systems would also counter an over-focus on providers of AI systems as the primary governance mechanism. The assumption, underpinned by the regulatory proposal, that AI providers can fix all potential issues related to the use of AI system largely reinforces the dominant role of large technology firms as AI providers, in particular to entirely determine the terms of public service provision. The AIA assigns the responsibility to detect and mitigate risks to fundamental rights and other possible harms to these private actors, regardless of whether or not they have the relevant expertise, resources, and vested interest to do so.

---

3   Ministrie van Binnelandse Zaken en Koninkrijksrelaties: Impact Assessment Mensenrechten en Algoritmes: https://www.uu.nl/sites/default/files/Rebo-IAMA.pdf
4   Speech by the Minister for Digitalisation, Alexandra van Huffelen, at 'AI and the future of Europe Brussels, 30 March 2022: https://www.rijksoverheid.nl/documenten/toespraken/2022/03/30/toespraak-alexandra-van-huffelen-30-maart-2022-brussel

----

<u>Amendments to the Artificial Intelligence Act</u>

The following amendments are designed to impose obligations on users of high-risk AI to ensure better foresight, transparency and accountability to those affected by the use of high-risk AI.

1. **Obligation on users of high risk AI to define affected persons**

2. **Include an obligation of users of high risk AI to conduct and publish a fundamental rights impact assessment,** detailing specific information to the context of use of that system, including the intended purpose, geographic and temporal scope, assessment of the legality and fundamental rights impacts of the system, compatibility with accessibility legislation, likely direct and indirect impact on fudnamental rights, any specific risk of harm likely to impact marginalised persons or those at risk of discrimination, the foreseeable impact of the use of the system on the environment, any other negative impact on the public interest; and clear steps as to how the harms identified will be mitigated, and how effective this mitigation is likely to be.