30-11-2021

An EU Artificial Intelligence Act for Fundamental Rights

A Civil Society Statement

The European Union institutions have taken a globally-significant step with the proposal for an Artificial Intelligence Act (AIA). Insofar as Artificial Intelligence (AI) systems are increasingly used in all areas of public life, it is vital that the AIA addresses the structural, societal, political and economic impacts of the use of AI, is future-proof, and prioritises the protection of fundamental rights and democratic values.

We specifically recognise that AI systems exacerbate structural imbalances of power, with harms often falling on the most marginalised in society. As such, this collective statement sets out the call of 114 civil society organisations towards an Artificial Intelligence Act that foregrounds fundamental rights. The statement outlines central recommendations to guide the European Parliament and Council in amending the European Commission's proposal for a Regulation,[1] published on the 21st of April 2021.

We, the undersigned organisations, call on the Council of the European Union, the European Parliament, and all EU member state governments to ensure that the forthcoming Artificial Intelligence Act achieves the following 9 goals:

1. A cohesive, flexible and future-proof approach to 'risk' of AI systems

The current form of the AIA's risk-based approach is dysfunctional. It delineates four levels of risk: unacceptable risk (Title II), high risk (Title III), systems that pose a risk of manipulation (Title IV), and all other AI systems. This approach of *ex ante* designating AI systems to different risk categories does not consider that the level of risk also depends on the context in which a system is deployed and cannot be fully determined in advance. Further, whilst the AIA includes a mechanism by which the list of 'high-risk' AI systems can be updated, it provides no scope for updating 'unacceptable' (Art. 5) and limited risk (Art. 52) lists. In addition, although Annex III can be updated

1 European Commission, Proposal for Regulation of the European Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final, 21 April 2021.

to add new systems to the list of high-risk AI systems, systems can only be added within the scope of the existing eight area headings. Those headings cannot currently be modified within the framework of the AIA. These rigid aspects of the framework undermine the lasting relevance of the AIA, and in particular its capacity to respond to future developments and emerging risks for fundamental rights.

To ensure a future-proof framework, we recommend that the AIA be amended to:

- **Introduce robust and consistent update mechanisms for 'unacceptable' and limited risk AI systems** so that the lists of systems falling under these risk categories can be updated as technology develops, using the same update mechanism currently proposed to add new high-risk systems to Annex III (see Title XI). This must allow new systems to be designated as posing unacceptable risk and therefore classified as prohibited practices (Title II, Art. 5), or as posing limited risk / risk of manipulation (Title IV, Art. 52) and therefore be subject to additional transparency obligations;
- **Include a list of criteria for 'unacceptable' and limited risk AI systems** under Arts. 5 and 52 respectively, to facilitate the updating process, provide legal certainty to AI developers and promote trust by ensuring that impacted individuals are protected against dangerous and potentially manipulative applications of AI;
- **Ensure that high-risk 'areas' (i.e. the eight area headings) listed in Annex III can be updated or modified under the Title XI mechanism** to allow for modifications to the scope of existing area headings, and for new area headings to be included in the scope of 'standalone' high-risk AI systems;
- **Expand Annex III** to include a more comprehensive list of high-risk systems, such as:
    - Expanding area heading 1 to all systems which use physical, physiological, behavioural as well as biometric data, including but not limited to biometric identification, categorisation, detection and verification;
    - Adding uses of AI for the purposes of conducting predictive analytics of migration;
    - Adding new area headings relating to healthcare and insurance.

2. Prohibitions on all AI systems posing an unacceptable risk to fundamental rights

Art. 5 of the AIA establishes the principle that some AI practices are incompatible with EU rights, freedoms and values, and should therefore be prohibited. However, in order for the AIA to truly prevent and protect people from the most rights-infringing deployments of AI, vital amendments are needed:

- **Remove the high threshold for manipulative and exploitative systems under Art. 5 (1)(a) and (b)** to prove that the systems operate *'in a manner that causes or is likely to cause that person or another person physical or psychological harm'*. The current framing erroneously implies that a person's behaviour can be materially distorted or exploited in a way that does not cause harm, whereas such practices are designed and/or used to undermine the essence of our autonomy, which is in itself an impermissible harm;
- **Expand the scope of Art. 5 (1)(b) to include a comprehensive set of vulnerabilities,** rather than limiting it to '*age, physical or mental disability*'. If an AI system exploits the vulnerabilities of a person or group based on any sensitive or protected characteristic, including but not limited to: age, gender and gender identity, racial or ethnic origin, health status, sexual orientation, sex characteristics, social or economic status, worker status, migration status, or disability, it is fundamentally harmful and therefore must be prohibited;
- **Adapt the Art. 5 (1)(c) prohibition on social scoring to extend to the range of harmful social profiling practices currently used in the European context.** The prohibition should be extended to also include private actors and a number of problematic criteria must be re-

moved, including the temporal limitation '*over a certain period of time*' and references to '*trustworthiness*' and '*single score';*

- **Extend the Art. 5 (1)(d) prohibition on remote biometric identification (RBI) to apply to all actors, not just law enforcement, as well as to both 'real-time' and 'post' uses**, which can be equally harmful. The prohibition should include putting on the market / into service RBI systems that are reasonably foreseeable to be used in prohibited ways. The broad exceptions in Art. 5(1)(d), Art. 5(2) and Art. 5(3) undermine the necessity and proportionality requirements of the EU Charter of Fundamental Rights and should be removed;
- **Prohibit the following practices that pose an unacceptable risk to fundamental rights under Art. 5:**
  - The use of emotion recognition systems that claim to infer people's emotions and mental states from physical, physiological, behavioural, as well as biometric data;
  - The use of biometric categorisation systems to track, categorise and / or judge people in publicly accessible spaces; or to categorise people on the basis of special categories of personal data, protected characteristics, or gender identity;
  - Systems which amount to AI physiognomy by using data about our bodies to make problematic inferences about personality, character, political and religious beliefs;
  - The use of AI systems by law enforcement and criminal justice authorities to make predictions, profiles or risk assessments for the purpose of predicting crimes;
  - The use of AI systems for immigration enforcement purposes to profile or risk-assess natural persons or groups in a manner that restricts the right to seek asylum and / or prejudices the fairness of migration procedures.

3. Obligations on users of high-risk AI systems to facilitate accountability to those impacted by AI systems

The AIA predominantly imposes obligations on '**providers'** (developers) rather than on '**users'** (deployers) of high-risk AI. While some of the risk posed by the systems listed in Annex III comes from how they are designed, significant risks stem from how they are used. This means that providers cannot comprehensively assess the full potential impact of a high-risk AI system during the conformity assessment, and therefore that users must have obligations to uphold fundamental rights as well.

To remedy this, we recommend that the AIA is amended **to include the following explicit obligations on users of high-risk AI systems**:

- **Include the obligation on users of high-risk AI systems to conduct a fundamental rights impact assessment (FRIA**) before deploying any high-risk AI system. For each proposed deployment, users must designate the categories of individuals and groups likely to be impacted by the system, assess the system's impact on fundamental rights, its accessibility for persons with disabilities, and its impact on the environment and broader public interest;
  - Preliminary assessments for users of non-high-risk AI systems should be encouraged, and support should be provided to users to properly determine risk level;
- **Include the obligation on users of high-risk AI systems to verify the compliance of the AI system with this Regulation** before putting the system into use;
- **Include the obligation on users to upload the information produced as part of the impact assessment to the EU database for stand-alone high-risk AI systems** (see Section 4 for more details).

4. Consistent and meaningful public transparency

The EU database for stand-alone high-risk AI systems (Art. 60) provides a promising opportunity for increasing the transparency of AI systems vis-à-vis impacted individuals and civil society, and could greatly facilitate public interest research. However, the database currently only contains information on high-risk systems registered by providers, without information on the context of use. This loophole undermines the purpose of the database, as it will prevent the public from finding out where, by whom and for what purpose(s) high-risk AI systems are actually used. Further, the AIA only mandates notification to individuals impacted by AI systems listed in Art. 52. This approach is incoherent because the AIA does not require a parallel obligation to notify people impacted by the use of higher risk AI systems under Annex III.

To ensure effective transparency, we recommend amending the AIA to:

- **Include an obligation on users to register deployments of high-risk AI systems in the Art. 60 database before putting them into use,** and include information in the database on every specific *deployment* of the system, including:
  - The identity of the provider and the user; the context and purpose of deployment; the designation of impacted persons; and the results of the impact assessment referred to in Section 3 above;
- **Extend the list of information that providers of high-risk AI systems must publish in the Art. 60 database** to include the information referred to in Annex IV point 2(b) and point 3, namely design specifications of the high risk AI systems (including the general logic, key design and optimisation choices);
- **Ensure the Art. 60 public database is user-friendly, freely accessible** (including for persons with disabilities)**, and navigable** (including by machines);
- **Extend the transparency obligations specified in Art. 52 to all high-risk AI systems**. Notifications presented to individuals should include the information that an AI system is in use, whom its operator is, general information about the purpose of the system, information about the right to request an explanation, as well as – in case of high-risk systems – a reference or link to the relevant entry in the EU database;
- **Remove the exemptions under Art. 52 for manipulative *'AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences***', as the use of manipulative AI systems in law enforcement and criminal justice contexts poses an acute risk to fundamental rights.

5. Meaningful rights and redress for people impacted by AI systems

The AIA currently does not confer individual rights to people impacted by AI systems, nor does it contain any provision for individual or collective redress, or a mechanism by which people or civil society can participate in the investigatory process of high-risk AI systems. As such, the AIA does not fully address the myriad harms that arise from the opacity, complexity, scale and power imbalance in which AI systems are deployed.

To facilitate meaningful redress, we recommend:

- **Include two individual rights in the AIA as a basis for judicial remedies:**
  - (a) The right not to be subject to AI systems that pose an unacceptable risk or do not comply with the Act; and
  - (b) The right to be provided with a clear and intelligible explanation, in a manner that is accessible for persons with disabilities, for decisions taken with the assistance of systems within the scope of the AIA;

- **Include a right to an effective remedy for those whose rights under the Regulation have been infringed** as a result of the putting into service of an AI system. This remedy should be accessible for both individuals and collectives;
- **The creation of a mechanism for public interest organisations to lodge a complaint with national supervisory authorities** for a breach of the Regulation or for AI systems which undermine fundamental rights or the public interest. This complaint should trigger an investigation into the system as outlined in Arts. 65 and 67.

6. Accessibility throughout the AI life-cycle

The AIA lacks mandatory accessibility requirements for AI providers and users. The proposal states that providers of non-high-risk AI systems *may* create and implement codes of conduct which *may* include voluntary commitments, including related to accessibility for persons with disabilities (Recital 81, Art 69. (2)).[2] This is an inadequate approach to disability and falls short of obligations laid out in the UN Convention on the Rights of persons with Disabilities (CRPD) and is inconsistent with existing EU legislation such as the European Accessibility Act. The lack of accessibility requirements risks leading to the development and use of AI with further barriers for persons with disabilities.

To ensure full accessibility for AI systems, we recommend:

- **The inclusion of horizontal and mainstreamed accessibility requirements for AI systems irrespective of level of risk,** including for AI-related information and instruction manuals, consistent with the European Accessibility Act.

7. Sustainability and environmental protections

The AIA misses a crucial opportunity to ensure that the development and use of AI systems can be done in a sustainable, resource-friendly way which respects our planetary boundaries. As a first step towards addressing environmental dimensions of sustainability, we need transparency about the level of resources needed to develop and operate AI systems.

To address this, we recommend:

- **The introduction of horizontal, public-facing transparency requirements on the resource consumption and greenhouse gas emission impacts of AI systems** – irrespective of risk level – in relation to design, data management and training, application, and underlying infrastructures (hardware, data centres, etc.).

8. Improved and future-proof standards for AI systems

The AIA is derived heavily from EU product safety legislation, and as such relies on the development of harmonised standards to facilitate providers' compliance with the Act. However, the AIA uses these technical standards to delegate key political and legal decisions about AI to the European Standardisation Organisations (Art. 3.27, Art. 40), which are opaque private bodies largely dominated by industry actors.

To ensure that political and fundamental rights decisions remain firmly within the democratic scrutiny of EU legislators, we recommend to:

2 Important issues such as environmental sustainability, stakeholders' participation in the design and development of AI systems, and diversity of development teams are also suggested in the AIA as merely voluntary measures.

- **Explicitly limit the harmonised standards established in Art. 40 (for Title III, Chapter 2, Requirements for high-risk AI) solely to genuinely technical aspects,** ensuring that the overall authority to set standards and perform oversight of all issues which are not purely technical, such as bias mitigation (Art. 10(2)(f)), remain in the remit of the legislative process;
- **Ensure that standards address the needs of all members of society via a universal design approach**. For example, to ensure that AI systems and practices are accessible for persons with disabilities, the standards harmonised for the AIA must be consistent with relevant standards harmonised for the European Accessibility Act, at a minimum;
- **Guarantee that relevant authorities, such data protection authorities and equality bodies, civil society organisations, SMEs and environmental, consumer and social stakeholders are represented and enabled to effectively participate in AI standardisation and specification-setting processes and bodies**;
- **Ensure that harmonisation under the AIA is without prejudice to existing or future national laws** relating to transparency, access to information, non-discrimination or other rights, in order to ensure that harmonisation is not misused or extended beyond the specific scope of the AIA.

9. A truly comprehensive AIA that works for everyone

Despite consistent documentation of the disproportionate negative impact AI systems can cause to already marginalised groups (in particular women*, racialised people, migrants, LGBTIQ+ people, persons with disabilities, sex workers, children and youth, older people, and poor and working class communities) significant changes are required to ensure that the AIA adequately addresses these systematic harms. To ensure the AIA works for everyone, we recommend to:

- **Ensure data protection and privacy for persons with disabilities.** The EU General Data Protection Regulation (GDPR) has rules that apply before processing special category data of persons who are 'physically or legally incapable of giving consent' (Art. 9(2)(c) of the GDPR) which may be insufficient to protect the rights of those persons in certain contexts relating to the use of AI:
  - **The AI Act must therefore ensure that privacy and data protection of all persons, including those under substituted decision-making regimes such as guardianships, are protected when their data are processed by AI systems**.
- **Remove the exemption for Large-scale EU IT systems in Art. 83.** Existing large-scale IT systems process vast amounts of data at a scale that poses significant risk to fundamental rights. No reasonable justification for this exemption from the AIA's rules is provided in the legislation or can be given:
  - **Any large-scale IT systems used by the EU must therefore be included in the scope of the AI Act through the deletion of the exclusion in section one of Art. 83.**
- **Equip enforcement bodies with the necessary resources.** While Art. 59 (4) emphasises the need to equip national authorities with 'adequate financial and human resources', according to the Explanatory Memorandum, the Commission currently only foresees 1 to 25 full-time equivalent positions per Member State for national supervisory authorities. This is clearly insufficient:
  - **The financial implications of the AIA must be reassessed and planned so as to ensure enforcement bodies and other relevant bodies have the resources to meaningfully fulfil their tasks under the AIA.**
- **Ensure trustworthy European AI beyond the EU.** Contrary to the objective of 'shaping global norms and standards for trustworthy AI consistent with EU values' as stated in the Explanatory Memorandum of the AIA, its rules currently do not apply to AI providers and users established in the EU when they affect individuals in third countries:

- **The AIA should ensure that EU-based AI providers and users whose outputs affect individuals outside of the European Union are subject to the same requirements as those whose outputs affect persons within the Union** to avoid risk of discrimination, surveillance, and abuse through technologies developed in the EU.

Drafted by: European Digital Rights (EDRi), Access Now, Panoptykon Foundation, epicenter.works, AlgorithmWatch, European Disability Forum (EDF), Bits of Freedom, Fair Trials, PICUM, and ANEC (European consumer voice in standardisation).

Signed by:

1. European Digital Rights (EDRi) (*European*)
2. Access Now (*International*)
3. The App Drivers and Couriers Union (ADCU) (*United Kingdom*)
4. Algorights (*Spain*)
5. AlgorithmWatch (*European)*
6. All Out (*International)*
7. Amnesty International (*International*)
8. ARTICLE 19 (*International*)
9. Asociación Salud y Familia *(Spain)*
10. Aspiration (*United States)*
11. Association for action against violence and trafficking in human beings - Open Gate / La Strada Macedonia (*North Macedonia*)
12. Association for Juridical Studies on Immigration (ASGI) (*Italy*)
13. Association for Monitoring Equal Rights (*Turkey*)
14. Association of citizens for promotion and protection of cultural and spiritual values - Legis Skopje (*North Macedonia*)
15. Associazione Certi Diritti (*Italy*)
16. Associazione Luca Coscioni (*Italy*)
17. Baobab Experience (*Italy*)
18. Belgian Disability Forum asbl (BDF) (*Belgium*)
19. Big Brother Watch (*United Kingdom)*
20. Bits of Freedom (*The Netherlands*)
21. Border Violence Monitoring Network (*European*)
22. Campagna LasciateCIEntrare (*Italy*)
23. Center for AI and Digital Policy (CAIDP) (*International)*
24. Chaos Computer Club (CCC) (*Germany*)
25. Chaos Computer Club Lëtzebuerg (*Luxembourg*)
26. CILD – Italian Coalition for Civil Liberties and Rights (*Italy*)
27. Controle Alt Delete (*The Netherlands*)
28. DataForGoodBCN (*Spain*)
29. DATAWO (*Greece*)
30. D3 - Defesa dos Direitos Digitais (*Portugal*)
31. D64 - Zentrum für digitalen Fortschritt (Center for Digital Progress) (*Germany*)
32. DataEthics.eu (*European*)
33. Digital Defenders Partnership (*International*)
34. Digitalcourage (*Germany*)
35. Digitale Freiheit e.V. (*Germany*)
36. Digitale Gesellschaft (*Germany*)
37. Digitale Gesellschaft (Schweiz) (*Switzerland*)
38. DIMMONS Digital Commons Research Group (*Spain*)
39. Disabled Peoples Organisations (*Denmark*)
40. DonesTech (*Spain*)

41. Državljan D / Citizen D (*Slovenia*)
42. Each One Teach One e.V. (*Germany*)
43. Elektronisk Forpost Norge (EFN) (*Norway*)
44. epicenter.works (*Austria*)
45. Equinox Initiative for Racial Justice (*European*)
46. Eticas Foundation (*Spain*)
47. Eumans (*European*)
48. European Anti-Poverty Network (*European*)
49. European Center for Not-for-Profit Law Stichting (*International)*
50. European Civic Forum (*European*)
51. European Disability Forum (EDF) (*European*)
52. European Network Against Racism (ENAR) (*European*)
53. European Network on Religion and Belief (*European*)
54. European Network on Statelessness (*European*)
55. European Sex Workers' Rights Alliance (*European*)
56. European Youth Forum (*European*)
57. Fair Trials (*European*)
58. FAIRWORK Belgium (*Belgium*)
59. FIDH (International Federation for Human rights) (*International*)
60. Fundación Secretariado Gitano (*Spain*)
61. Future of Life Institute (*International*)
62. GHETT'UP (*France*)
63. Greek Forum of Migrants (*Greece*)
64. Greek Forum of Refugees (*European*)
65. Health Action International (*The Netherlands*)
66. Helsinki Foundation for Human Rights (*Poland*)
67. Hermes Center (*Italy*)
68. Hivos (*International*)
69. Homo Digitalis (*Greece*)
70. Human Rights Association (*Turkey*)
71. Human Rights House Zagreb (*Croatia*)
72. HumanRights360 (*Greece / European*)
73. Human Rights Watch (*International*)
74. ILGA-Europe - The European Region of the International Lesbian, Gay, Bisexual, Trans and Intersex Association (*European*)
75. Implementation Team of the Decade of People of African Descent (*Spain*)
76. info.nodes (*Italy*)
77. Interferencias (*Spain*)
78. International Commission of Jurists (NJCM) - Dutch Section (*The Netherlands*)
79. Irish Council for Civil Liberties (ICCL) (*Ireland)*
80. IT-Pol Denmark (*Denmark*)
81. JustX (*European*)
82. JustPeace Labs (*International*)
83. KOK - German NGO Network against Trafficking in Human Beings (*Germany*)
84. Lafede.cat – organitzacions per a la justícia global (*Spain*)
85. Ligue des droits de l'Homme (LDH) (*France*)
86. Ligue des droits humains (*Belgium*)
87. Maruf Foundation (*The Netherlands*)
88. Mediterranea Saving Humans Aps (*Italy / International)*
89. Melitea (*European*)
90. Mnemonic (*Germany / International*)
91. Moje Państwo Foundation (*Poland*)
92. Montreal AI Ethics Institute (*Canada*)

93. Movement of Asylum Seekers in Ireland (MASI) (*Ireland*)
94. Movimento SOS Racismo (*European*)
95. Netwerk Democratie (*The Netherlands*)
96. NOVACT (*Spain / International*)
97. OMEP - Oraganisation Mondiale pour l'Education Prescolaire / World Organization for Early Childhood Education (*International*)
98. Open Knowledge Foundation (*International*)
99. Open Society European Policy Institute (OSEPI) (*International*)
100. OpenMedia (*International*)
101. Panoptykon Foundation (*Poland*)
102. The Platform for International Cooperation on Undocumented Migrants (PICUM) (*International*)
103. Privacy International (*International*)
104. Privacy Network (*Italy*)
105. Racism and Technology Center (*The Netherlands*)
106. Ranking Digital Rights (*International*)
107. Refugee Law Lab, York University (*International*)
108. Refugees in danger (*Denmark*)
109. Science for Democracy (*European*)
110. SHARE Foundation (*Serbia*)
111. SOLIDAR & SOLIDAR Foundation (*European*)
112. Statewatch (*European*)
113. Stop Wapenhandel (*The Netherlands*)
114. StraLi (*European*)
115. SUPERRR Lab (*Germany*)
116. Symbiosis-School of Political Studies in Greece, Council of Europe Network (*Greece*)
117. Taylor Bennett Foundation (*United Kingdom*)
118. UNI Europa (*European)*
119. Universidad y Ciencia Somosindicalistas (*Spain*)
120. Vrijschrift.org (*The Netherlands*)
121. WeMove Europe (*European*)
122. Worker Info Exchange (*International*)
123. Xnet (*Spain)*

Supporters:

1. Cities Coalition for Digital Rights (*European*)

* This statement outlines the baseline agreement amongst the signatory civil society organisations on the EU's proposed Artificial Intelligence Act. However, some of the signatories have positions that are in places more specific and extensive than those outlined here; this statement does not serve to limit this in any way.