European Center for Not-for-Profit Law

European Artificial Intelligence & Society Fund

Towards an AI Act that serves people and society

Strategic actions for civil society and funders on the enforcement of the EU AI Act

August 2024

A report prepared for the European AI & Society Fund by the European Center for Not-for-Profit Law (ECNL)

https://europeanaifund.org/

Contact:
info@europeanaifund.org

Network of European Foundations
Rue Royale 94
1000 Brussels, Belgium

Authors:
Karolina Iwańska, ECNL
Vanja Skoric, ECNL
Francesca Fanucci, ECNL
Berna Keskindemir, ECNL
Sushruta Kokkula, ECNL

Editor:
Catherine Miller, European AI & Society Fund

Acknowledgements:
Members of the #ProtectNotSurveil Coalition, members of the AI Coalition coordinated by European Digital Rights (EDRi), Members of EDRi Platform Working Group, Eliška Pírková, Asha Allen, Jan Penfrat, Julian Jaursch

Design:
Marta Posada

Table of Contents

Executive Summary

The coming two years will be critical for the future of Artificial Intelligence regulation in Europe. While the adoption of the European Union's AI Act in 2024 was a significant achievement in itself, the implementation and enforcement phase that now follows will decide whether it can have a practical impact on how AI is developed and used. Public interest advocates must be active partners in this process to ensure that the regulation can be an effective tool to challenge the harmful impacts of AI on society and secure accountability over AI use. Their success will determine the future direction of AI not just in Europe, but also in the many countries across the globe that look set to follow the EU's regulatory lead.

This report, commissioned by the European AI & Society Fund and carried out by the European Center for Not-for-Profit Law (ECNL), identifies opportunities for civil society to shape the outcomes of the AI Act over this period. It describes the different stages of implementation, suggests specific activities civil society can undertake, the skills and expertise required, and what funders can do to support this work.

In the months ahead, the institutions that will operationalise the AI Act will be established, the guidelines that specify prohibitions and risks will be drawn up, transparency measures will be drafted and technical standards agreed. With civil society participation, each of these presents an opportunity to implement the Act in line with the public interest, uphold fundamental rights and protect the most vulnerable. This could ensure that bans on the most harmful AI systems, like remote biometric identification (RBI), are

This could ensure that bans on the most harmful AI systems, like remote biometric identification (RBI), are tightly drawn, that products like ChatGPT have to address the systemic risks they pose to society, and that exemptions around national security and migration are limited.

tightly drawn, that products like ChatGPT have to address the systemic risks they pose to society, and that exemptions around national security and migration are limited. Without civil society pushback, these processes are an opportunity for industry to slacken rules and widen loopholes, limiting the final effectiveness of the law.

This period is also a time to prepare to apply the law in practice. The AI Act is complex and sits within a mosaic of established fundamental rights and equalities legislation as well as freshly passed digital markets regulation. Navigating routes to accountability will require the painstaking preparation of test cases, which will be the essential test of the EU's claim to be the home of trustworthy AI.

Recent experience from the Digital Services Act (DSA) demonstrates that civil society can have tangible impact by shaping the implementation of a law, and work alongside regulators to start holding companies to account. It also highlights the need for skills and resources to make this happen.

We have summarised below the most important capacities civil society will need for the implementation and enforcement of the AI Act, and recommendations for how funders can support this.

Drawing on these lessons, which are explored at the end of the report, we have summarised below the most important capacities civil society will need for the implementation and enforcement of the AI Act, and recommendations for how funders can support this. The report then goes on to describe in detail the opportunities for engagement with the new institutions that govern the AI Act, specific provisions of the Act that hold scope for civil society influence, and how public interest advocates can leverage standardisation procedures and strategic litigation. Each of these are prioritised by urgency and include suggested activities to achieve impact.

These recommendations are based on ECNL's analysis of the AI Act and engagement with the field. They are offered as a starting point for further discussion and strategising, both among public interest advocates and the funders that support them, and we welcome feedback to refine and improve them. The European AI & Society Fund is developing its grantmaking informed by these recommendations and in dialogue with our communities.

Recommendations

Civil society coordination

Given the scarce resources available, it's essential that civil society leverages individual organisations' unique strengths and collaborates on a collective approach to the implementation and enforcement process.

It's an urgent priority to demand and establish clearly structured coordination mechanisms for civil society organisations (CSOs) to engage with the relevant institutions, namely the AI Office, the European Data Protection Supervisor (EDPS) both at EU level and with the national market supervisory bodies in the Member States. In particular, there needs to be a coordinated approach to advocating for, and then nominating, civil society members of the Advisory Forum, as well as fundamental rights experts to the Scientific Panel.

Coordination mechanisms between groups working at EU level and national level will also be required during implementation and beyond. Additional coordination will be needed for groups providing input into technical standards and those working on strategic litigation, while the #ProtectNotSurveil coalition needs to sustain and build its coordination around migration issues.

What funders can do

Provide dedicated funding to resource coordination across the civil society community and for specific focus areas like migration, technical standards and litigation.

Commit to providing financial support to CSOs whose representatives are selected to participate in the advisory forum or the scientific panel and to resource their coordination with the wider community.

Provide opportunities for knowledge and skills exchange between national and EU-level CSOs.

Research

Research capacity will be needed across many areas of the implementation and enforcement process. Some of this will require technical skills that are outside the current expertise of many of the CSOs active in this field.

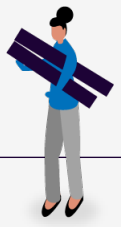
Evidence building will be needed as a foundation for advocacy around the prohibitions, risk designations and exemptions of the AI Act, including mapping AI systems that should be fully banned or categorised as high risk, those used for national security purposes and in the context of migration. This evidence will need to be accompanied by fundamental rights-based legal analysis.

It will also be necessary to develop a taxonomy of the systemic risks of general-purpose AI (GPAI) and map existing GPAI models that present these characteristics.

Drawing on academic expertise, research will also be required to identify the elements necessary for Fundamental Rights Impact Assessments (FRIAs) and the transparency database to be effective instruments.

Further research and legal analysis will be needed to understand how the AI Act can be combined with existing tools such as equalities legislation and the GDPR to create routes to accountability. This should focus on identifying test cases that can be brought once the Act is in force.

And once the AI Act is in force, research will be required to monitor the public EU database to identify AI systems which have been wrongly exempted from AI Act obligations and explore high-risk AI systems that could be cases for litigation, campaigning or advocacy.



What funders can do

Provide financial support to organisations for research capacity.

Foster connections between academic experts and CSOs.

Identify technical experts who are willing and available to work with CSOs, for example by establishing a network of public interest technologists, and "matching" experts with (groups of) CSOs on well-defined tasks.

Advocacy

The success of any advocacy will be strongly dependent on the strength of civil society coordination and the existence of a robust research foundation for public interest arguments (see above). Advocacy strategies must also be coherent with wider civil society approaches to political and legislative developments, particularly in the areas of migration, policing and surveillance.

Priorities for EU level advocacy will be:

- Shaping **guidelines on prohibitions** in line with fundamental rights and ensuring exceptions are interpreted narrowly.
- Establishing **guidelines on high-risk AI systems** which limit the scope for exemptions from AI Act requirements.
- Adopting a public interest-focused **code of practice on GPAI** and pushing for the designation of systems that pose systemic risk.
- Pushing for a **FRIA** template and **EU transparency register** that meets the criteria identified in the research phase to provide effective visibility and oversight of AI systems used in Europe (see above).
- Demanding meaningful **transparency measures** towards people subject to the use of AI where the Act requires it and pushing to extend these measures to other areas.

Priorities at national level will be:

- Supporting Member State governments that want to impose stronger limits on **RBI systems** than the AI Act foresees, and fighting national level legislation with weaker provisions.
- Pushing for national legislation that could strengthen fundamental rights protections around **national security, law enforcement and migration.**
- Demanding that market surveillance authorities in Member States and the EDPS at the EU level provide feedback to complainants that use the AI Act's **redress mechanisms**.

There are also some opportunities for direct engagement with industry, for example by encouraging companies to voluntarily adopt more stringent measures, allowing greater stakeholder engagement than the AI Act foresees or adopting the AI Act's requirements beyond the EU.

What funders can do

Continue providing funding for organisations that have been active advocates in the legislation's development through the implementation and enforcement phase.

Support national level CSOs in monitoring the appointment of national authorities and their independence based on an assessment of the country's significance.

Commission research mapping national-level enforcement structures in all Member States, once all national competent authorities are established.

Strategic litigation

In the short term, there is a time-bound and politically sensitive possibility of challenging provisions of the AI Act around national security exemptions and the failure to impose a full ban on RBI at the Court of Justice of the European Union (CJEU). These would require cooperation from a Member State which is unlikely.

Aside from this, strategic litigation work will require research (see above) to identify the most fruitful avenues to pursue and the different legal instruments that can be deployed. It is likely to focus on identifying and bringing cases around AI systems which should be covered by the AI Act's prohibitions, particularly on RBI systems, as well as cases challenging the scope of the national security exemption.

What funders can do

Support coordination among CSOs interested in pursuing strategic litigation.

Identify litigation experts (including from adjacent fields) who can provide support on developing strategies.

Provide financial support for a number of test cases to be launched once the AI Act comes into force.

Campaigning and movement building

While implementation and enforcement are primarily a technical and detailed process, there's nonetheless a need for pressure on responsible authorities to ensure that the public interest remains a priority. There's a specific opportunity for mobilisation around a full ban on RBI, building on the existing Reclaim Your Face campaign, particularly in countries where there are moves to introduce legislation authorising RBI.

Transparency requirements within the AI Act also hold the potential to reveal use cases of AI that could be the focus of future campaigns. This will require coordination with the research capacity described above.

What funders can do

Provide financial support to campaigning organisations, particularly around RBI, national security and migration.

Support coordination between campaigners and other CSOs, including building connections with adjacent groups such as People vs. Big Tech and the Better Information Project.

Support coordination between campaigners across different Member States around RBI measures.

Underpinning all these recommendations is the urgent need to map which groups are already active, which work is already resourced and where there are gaps in critical skills, expertise and specific geographies. With this analysis, funders can not only direct resources effectively but can also help bridge the different activities, amplifying their impact. Additionally, they can provide spaces for strategy, learning and exchange across these areas and build relationships with external stakeholders like technical experts, journalists or industry.

It is also important to note the urgency of the implementation timeline – many of the activities described are already under way, often despite insufficient resourcing for civil society. Funders should consider making ad hoc "emergency" support available outside the usual grantmaking cycles to ensure the most immediate needs are addressed.

Above all, in resourcing capacities, attention must be paid to ensure that the community remains diverse and those most affected by the impacts of AI are at the forefront of the civil society response. Funders should also consider concerns related to longtermist/ effective altruism groups and their potential to shift attention away from the existing, real-life harms of AI.

Introduction and context

The European Union adopted the AI Act in 2024 after a three-year period of legislative development. It is globally the most advanced attempt to regulate Artificial Intelligence technologies. Its primary objective is to establish harmonised regulations governing AI development and use within the EU while upholding fundamental rights, and to strike a balance between encouraging innovation and addressing societal impacts. EU regulations have a significant impact on global policy and legislative efforts, and the AI Act is set to amplify this effect. Countries across the globe are beginning to copy the AI Act, with uncertain results.

Despite vigorous advocacy from civil society organisations (CSOs) which succeeded in securing some significant improvements during the development of the law, many are disappointed with the final text. It is riddled with far-reaching exceptions which lower protection standards, especially in law enforcement and migration. Nonetheless, the AI Act establishes a mandatory framework which, if properly implemented, is a real opportunity to improve transparency and accountability of how AI systems are developed and deployed, especially in the public sector. The Act largely relies on secondary legislation (e.g., delegated and implementing acts, codes of practice, templates and technical standards) to translate its requirements into concrete processes and benchmarks. These implementing documents will be crucial for ensuring AI accountability in practice, notably to ensure that gaps left by the AI Act are interpreted narrowly and do not lead to further watering down of fundamental rights protections.

How the AI Act works

The Act is a risk-based regulation with four levels: unacceptable, high, limited and minimal, plus an additional category for general-purpose AI (GPAI). There are prohibitions on applications with unacceptable risks, and high-risk applications must comply with security, transparency and quality obligations, and undergo conformity assessments. Limited-risk applications only have transparency obligations, while minimal-risk applications are not regulated. There are separate rules for GPAI which include transparency requirements and additional evaluations for high-capability models.

The AI Act creates distinct obligations for AI providers and AI deployers. For the purposes of this document, these terms should be understood as follows:

- **AI providers:** an individual or company, public authority, agency or other body that **develops** an AI system or a GPAI model (or that commissions this development) and makes it available on the EU market (for sale or use) under its own name or trademark, whether for payment or free of charge.
- **AI deployers:** an individual or company, public authority, agency or other body **using** an AI system under its authority. This does not apply to personal, non-professional use.

Examples **welfare risk assessment system:**

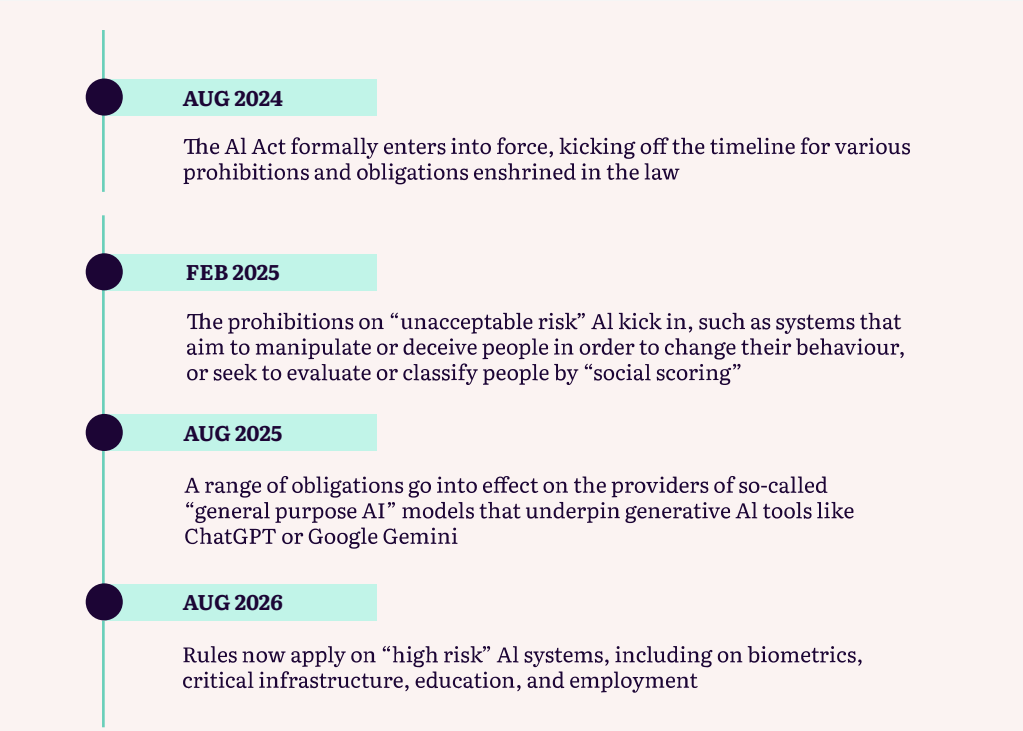
1. Company A develops a risk assessment system and sells it to several municipalities in one or multiple countries. Company A is the provider and individual municipalities are deployers.
2. The municipality of Amsterdam commissioned a risk assessment system from Company A. The system is not made available on the market to be bought by others and it is used under the name of the municipality. It is the municipality's responsibly to ensure that both the provider and deployer obligations are fulfilled.
3. The municipality developed the system in-house. The municipality has to fulfil both the provider and deployer obligations.

The AI Act will be operationalised by a multifaceted governance framework involving various entities, including the European AI Board, the European AI Office and national competent authorities, as well as advisory and expert bodies, such as the advisory forum and the scientific panel.

Timeline

The AI Act will come into force in phases, with almost full application anticipated by 2026 (see timeline below).

Enforcement timeline



Source: Financial Times.

In Annex I, we present a comprehensive mapping of all implementation processes explicitly mentioned in the AI Act, together with an indication of the responsible authority, timeline and recommendations for necessary contributions from civil society. We hope that this will serve as a useful compass for a wide range of organisations interested in participating in the implementation of the AI Act, either on the EU or the national level.

The role of civil society

We particularly encourage those with social justice expertise and that represent those most affected by AI to shape the civil society response to the AI Act, recognising that the negative societal impacts of Artificial Intelligence are often experienced most acutely by people and communities that have been marginalised.

Throughout this report we identify opportunities for civil society to influence the implementation and enforcement of the AI Act. We recognise that civil society is a broad term that can include a wide range of actors representing diverse perspectives.

When we refer to civil society, we mean individuals and organisations that act in the public interest, specifically those that fight to secure fundamental rights, challenge social injustice and promote fair, inclusive and sustainable societies. We particularly encourage those with social justice expertise and that represent those most affected by AI to shape the civil society response to the AI Act, recognising that the negative societal impacts of Artificial Intelligence are often experienced most acutely by people and communities that have been marginalised.

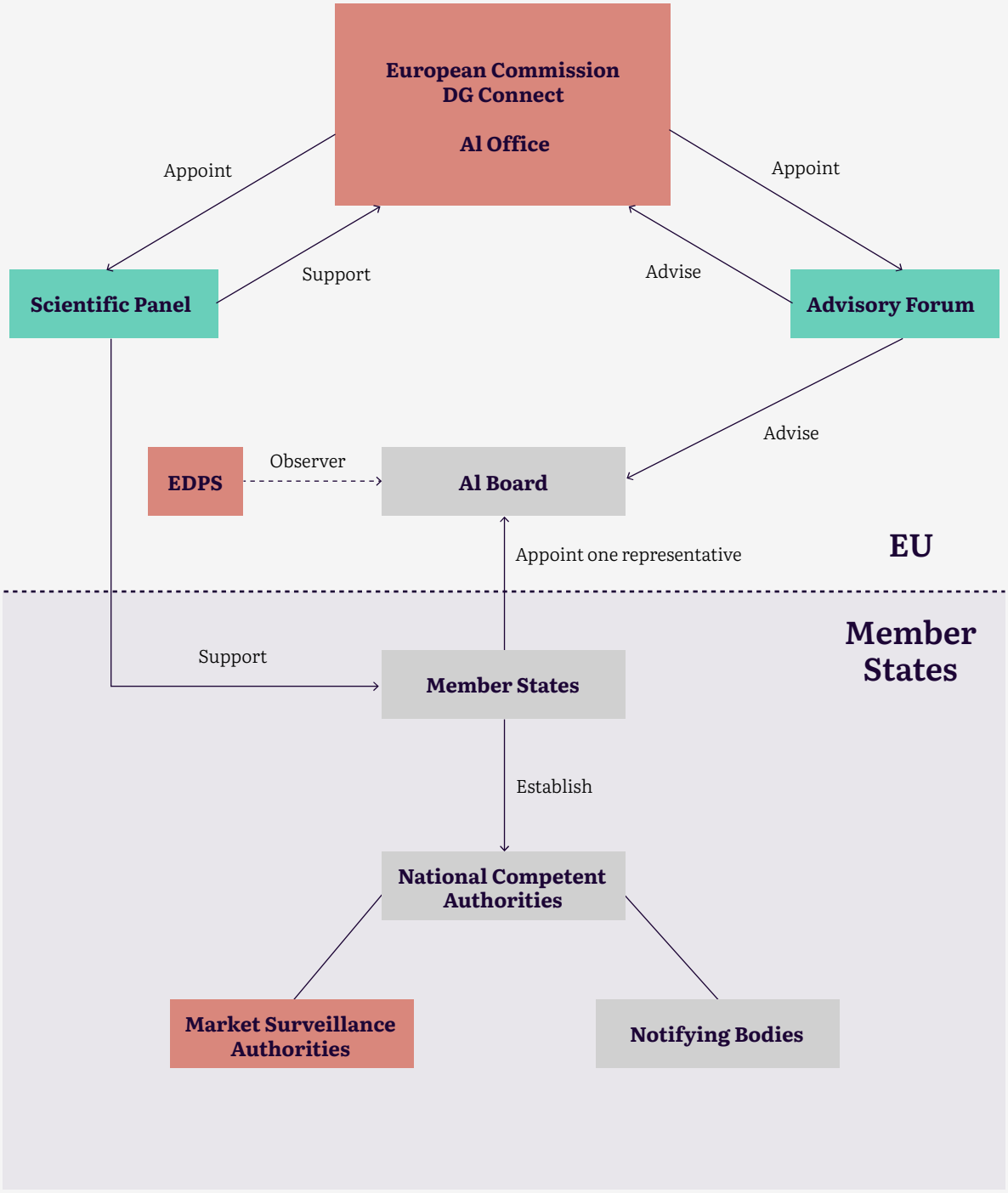
There are currently a number of organisations active in the EU policy debate that promote longtermist views and focus on "existential" harms of AI which shift policymakers' attention away from existing, real-life harms. Likewise, there are organisations that are largely backed by corporate interests. We caution the EU and Member State institutions to meaningfully engage with the widest possible range of civil society actors, in particular those promoting and actively working on fundamental rights, in order to fulfil the spirit of the AI Act and adhere to the founding values of the European Union.

The AI Act introduces an elaborate framework, where various bodies contribute to the implementation and enforcement of the law. National-level market surveillance authorities ensure that AI systems available on the EU market fulfil relevant requirements. Meanwhile, EU bodies have responsibility for AI systems used by EU institutions and some specific responsibilities for general-purpose AI (GPAI), as well as oversight of the overall implementation of the law. To secure effective implementation of the AI Act, it will be important for civil society to establish relationships within the different bodies early on and use opportunities for public interest representation where they exist.

How governance in the AI Act works

Competent authorities will be set up or designated in each Member State with the power to impose fines for non-compliance with the AI Act at national level. The European Data Protection Supervisor (EDPS) and the European Commission (through the newly established AI Office) will be the responsible authorities at EU level. Additional bodies will be set up at EU level to support, advise, monitor, provide expertise and harmonise enforcement action.

Overview of AI Act enforcement and oversight institutions



Source: ECNL

National level		EU level
National competent authorities	**European Data Protection Supervisor (EDPS)**	**AI Office**
Has the competence to supervise:		
AI systems put on the market by **providers** based in that country.	All EU institutions, bodies and agencies **developing or deploying** AI systems, e.g., the European Commission, Frontex, Europol, Eurojust etc.	AI systems based on GPAI models where both the model and the system are **provided by the same entity**, e.g., ChatGPT.
AI systems put on the market by **non-EU providers** who set up an authorised representative in that country.		
AI systems **deployed** in that country, be it by a public authority or a company.		
GPAI systems embedded in high-risk systems **deployed** in that country (in cooperation with the AI Office).		
Main powers:		
• Request documentation. • Conduct unannounced on-site and remote investigations. • Access source code during investigations. • Receive reports for law enforcement about the use of remote biometric identification systems. • Request assistance from the scientific panel of independent experts.		• Monitor the market, also with the view of updating the law. • Ex-post evaluation of GPAI systems. • Request assistance from the scientific panel of independent experts or the advisory forum.

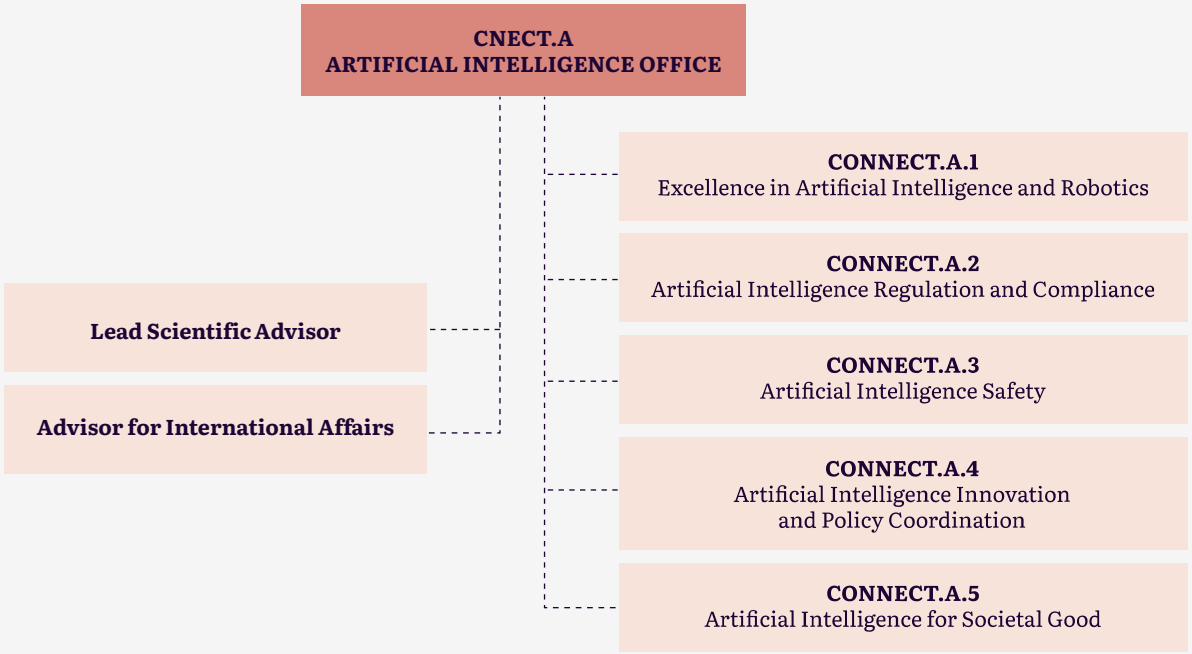
Examples	Competent forum:
Polygraph developed by an American company whose representative is based in Ireland that is later purchased and used by Polish border guard.	Ireland for the provider. Poland for the deployer. Coordination and harmonisation via the AI Board.
Polygraph developed by a French company that was procured and is put into use by Frontex.	France for the provider. EDPS for Frontex.
A school in Slovenia that has embedded a custom version of ChatGPT into a system that they use.	Slovenia, in collaboration with the AI Office.

Opportunities for civil society engagement with the institutions

1. European Commission and the new EU AI Office

The European Commission has overall responsibility for the effective implementation of the AI Act. It will issue delegated acts and guidelines, establish relevant bodies and appoint their members as well as conduct evaluations of the AI Act.

The European AI Office is being set up within DG Connect with an expected staff of around 140 to develop EU capabilities on AI and support the implementation and enforcement of the Act. The AI Office also has a specific remit to enforce provisions of the AI Act around GPAI where both the AI model and the system are developed by the same entity (e.g., ChatGPT).



Source: European Commission

For the most urgent implementation issues, CONNECT.A.2 (previously responsible for the development of the AI Act), led by Kilian Gross, will be the most important unit of the AI Office. Unit CONNECT.A.3 will be crucial for organisations interested in GPAI systems, including the development of codes of conduct. Materials made available by the Commission indicate the Office is planning to recruit legal experts but there is no specific requirement for it to include in-house expertise on fundamental rights. It will, however, engage with other stakeholders where there is an opportunity for public interest and human rights input, including consultations with experts from the scientific community, the educational sector, citizens, civil society, and social partners, and cooperation with DG JUST and other EU bodies, including the EU Fundamental Rights Agency and the EDPS and Board, and international cooperation.

Recommendations for engagement

High priority (2024)

- Establish coordination mechanisms among the CSO community to work collectively with the AI Office, identifying key individuals responsible for specific implementation activities and coordinating ways to provide input.
- Advocate for the establishment of clear structures for cooperation and regular consultation with CSOs and fundamental rights experts (i.e., organise a meeting in the second half of 2024 between a group of CSOs and the head and key staff of the AI Office, focused specifically on civil society engagement, rather than substantive issues.)

Medium priority (2025):

- Engage with other institutions that are AI Office stakeholders and push for structures for input which can then be relayed by them to the AI Office.
- Identify allies in other stakeholder groups with a shared need for engagement, such as consumer groups, trade unions, investors, and potentially also companies.

2. European Data Protection Supervisor (EDPS)

The EDPS will be the market surveillance authority for EU bodies, institutions and agencies. This means that it will have the same enforcement powers towards EU institutions that develop or deploy AI systems as national market surveillance authorities do for national-level actors. The EDPS is already responsible for the enforcement of data protection rules vis-à-vis EU bodies. In the development of the AI Act it issued several recommendations to EU legislators to ensure the protection of fundamental rights, e.g., calling for a full prohibition of RBI.

Recommendations for engagement

High priority (2024)

- Advocate for the establishment of clear structures for cooperation and regular consultation with CSOs and fundamental rights experts, in particular to flag concerns regarding the use of AI systems by EU bodies.

3. European AI Board

Article 65 of the AI Act sets up the European AI Board to ensure consistent and effective application of the AI Act, including by coordinating and providing guidance for harmonisation practices, sharing best practices among Member States, and providing advice on implementation, especially on GPAI. It is comprised of Member States representatives, appointed for three years. The AI Office is the Board's secretariat and can attend meetings but not vote. The EDPS can attend meetings as an observer. There is no specific requirement for fundamental rights expertise within the Board itself but it is tasked with cooperating with relevant EU institutions and other networks in the field of fundamental rights.

Recommendations for engagement

Medium priority (2025)

- Advocate for a standing sub-group of the Board focused specifically on fundamental rights, with regular participation from civil society members of the Advisory Forum (see below) and input from external CSO experts.
- Establish civil society coordination mechanisms to feed into meetings of this sub-group.

4. Advisory Forum

Article 67 of the AI Act sets up the Advisory Forum to provide technical expertise and advise the AI Board and the Commission. This creates a formalised opportunity for engagement as it comprises a range of stakeholders, including civil society as well as industry, start-ups, SMEs and academia. Balance has to be ensured between commercial and non-commercial interests. Members are appointed by the European Commission for two years, with the possibility of extending to a maximum of four years. There are five permanent institutional members: the Fundamental Rights Agency and the EU technical/standardisation bodies (ENISA, CEN, CENELEC, ETSI). According to the Commission, technical expertise should be understood not only as expertise in computer science, but also expertise in AI's impacts on fundamental rights and society. However, there is no specific requirement to include fundamental rights expertise among its members.

Recommendations for engagement

High priority (2024)

- **Urgent:** Advocate with the European Commission for clear criteria for the selection of members, explicit inclusion of fundamental rights expertise, and a specified number of seats dedicated for civil society representatives, equal to that of other stakeholders. An important consideration will be the definition of civil society, specifically to prevent seats being claimed by organisations which are not grounded in fundamental rights (e.g., "longtermist" organisations) or those primarily funded by tech companies.

  | ECNL, Access Now and the Irish Council for Civil Liberties (ICCL) are already engaging with the Commission. Further support (e.g., open letters, media coverage) might be necessary to put public pressure on the Commission, especially to ensure an equal number of seats for civil society.

- Apply as candidates or support nominations of other CSO representatives (likely October-November 2024).

  | Coordinate on the application process, depending on the membership structure proposed by the Commission.

Medium priority (2025)

- Establish coordination mechanisms between civil society representatives on the advisory forum and the broader CSO community.
- Advocate for regular consultation of the forum with CSOs and fundamental rights experts that are not formal members of the forum.

5. Scientific panel of independent experts

Article 68 of the AI Act sets up the Scientific Panel to advise the AI Office on GPAI models and systems and support market surveillance authorities at the national level or in cross-border activities, at their request. For example, the scientific panel may provide a "qualified alert" to the AI Office if it suspects that a general-purpose model should be classified as posing systemic risks. It will be made up of independent experts selected by the Commission on the basis of up-to-date scientific or technical expertise in the field of AI. In line with Art. 68(1), the Commission should issue an implementing act establishing the scientific panel and setting out rules for the selection of members, including for ensuring fair gender and geographical representation. At the time of publication this implementing act has not yet been adopted.

Recommendations for engagement

High priority (2024)

- Advocate for selection criteria to also include members with human rights, sociology, and interdisciplinary (e.g. Science and Technology Studies) expertise, as well as for cooperation and regular consultation by the panel with CSOs and human rights experts. Explore alliances with the academic community to support these recommendations.
- Prepare to engage with the panel by nominating members or supporting nominations of other experts. At this point the timeline for appointments is not clear.

Medium priority (2025)

- Establish coordination mechanisms among the CSO community to provide input to scientific panel members.

6. National competent authorities

Under the AI Act each Member State must establish at least one market surveillance authority with powers to enforce the legislation and ensure that only products that comply with the AI Act are available on the EU market. Depending on the country, the market surveillance authorities are expected to be a mix of existing data protection authorities, sectoral authorities (e.g., financial oversight agencies) and newly established bodies. Additionally, Member States must set up a notifying authority to monitor third-party conformity assessments. However, under the AI Act conformity will be conducted by self-assessment in the majority of aspects and third-party assessments will only be required for high-risk AI systems involving biometrics.

While the process of appointing authorities is still at an early stage, there are already concerning developments in Member States (Italy, Denmark) whose appointed authorities fail to meet the AI Act's independence and impartiality requirements, as they are politically and governmentally dependent. Separately to this report, ECNL has published two case studies of how the national authorities are likely to take shape in Spain and the Netherlands, which indicate some of the different approaches that could be taken.

Recommendations for engagement

High priority (2024)

- National-level CSOs should monitor the setting up of competent authorities, particularly in relation to their independence, and flag concerns to the relevant EU institutions.
- Brussels-based CSOs should advocate with the Commission to keep Member States accountable in this regard (see the open letter by Access Now, the European Consumer Organisation (BEUC) and the Hermes Center, sent to the Commission and Member States).

Medium priority (2025)

- Advocate for the establishment of clear structures for cooperation and regular consultation with CSOs and fundamental rights experts. This could include national versions of the advisory forum that engages with the EU AI Office. There is already some precedent in Germany, where the Digital Services Coordinator responsible for the Digital Services Act (DSA) enforcement set up a multi-stakeholder advisory body.
- Set up an accessible database of all authorities appointed in Member States as well as options for external engagement with those bodies.

7. National human rights institutions

Article 77 of the AI Act gives national human rights institutions the right to access documentation produced by the provider or developer of an AI system where it is necessary for them to fulfil their mandate to protect fundamental rights. Advice to the Dutch government indicated that these institutions should also flag breaches in fundamental rights law to the market surveillance authority and support the market surveillance authority to build its own understanding of the fundamental rights risks that AI can pose. Doing this would require a cooperation structure between the fundamental rights bodies and market surveillance authorities. This advice could form the basis of civil society advocacy across other Member States.

Recommendations for engagement

High priority (2024)

- National-level CSOs, especially in the largest countries like Germany and France, should identify all relevant institutions that should be appointed as bodies responsible for the protection of fundamental rights in line with Article 77. This is understood to be underway in Germany by consumer groups, but should not be limited to consumer rights and should also be undertaken elsewhere.
- Civil society should establish relationships with these bodies and encourage them to push to be designated institutions under the Act.
- Civil society should advocate with national governments to ensure that all relevant bodies are designated to be able to use the powers granted by Art. 77.

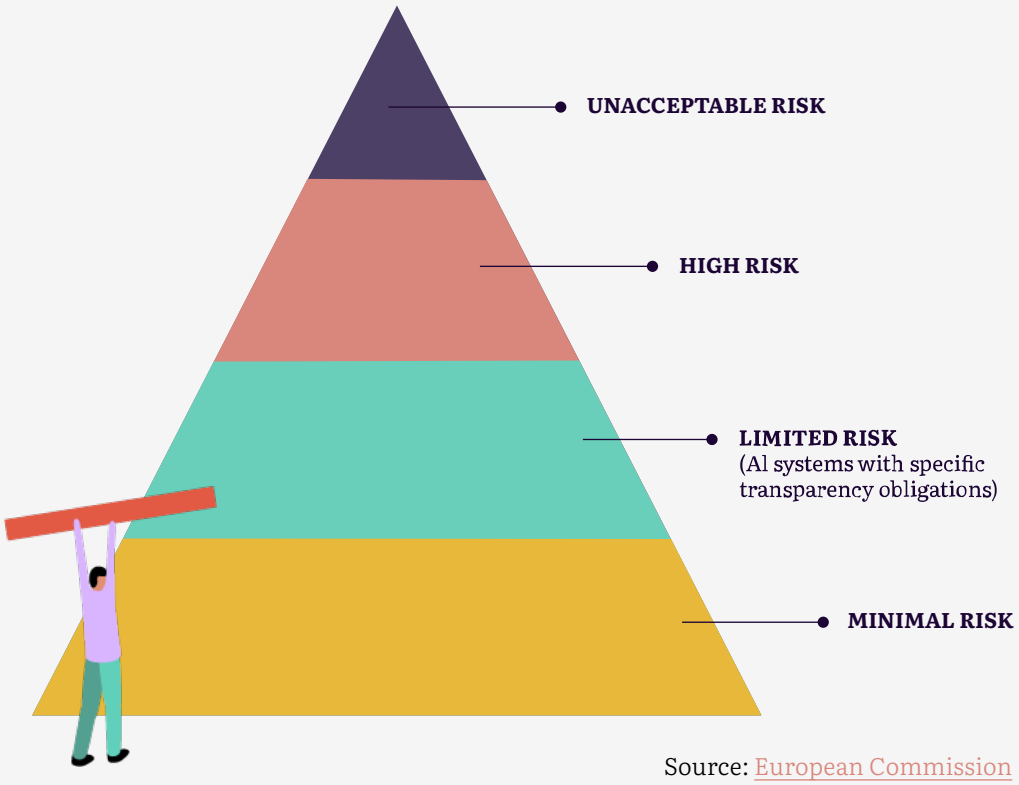
Key AI Act provisions for civil society engagement

The AI Act relies on a risk-based approach, where safeguards vary depending on the level of risk to health, safety and fundamental rights. AI systems deemed to pose "unacceptable" risk cannot be developed and used in the EU. Most of the AI Act requirements apply only to the category of "high-risk" systems. Finally, some additional AI systems have specific transparency obligations.

This section highlights the provisions of the AI Act with most relevance to the protection of fundamental rights. The effectiveness of these provisions will depend on how they are interpreted and implemented – it will be civil society's job over the next two years to fight for a robust approach.

Additionally, we highlight the cross-cutting issue of migration where there are significant loopholes that need to be addressed.

AI Act defines 4 levels of risk for AI systems:



Source: European Commission

Prohibitions: Article 5

Article 5 of the AI Act introduces a list of prohibited systems that cannot be developed, sold or used in the EU. This provision is a major win for civil society advocacy as it explicitly introduces red lines for systems that are incompatible with fundamental rights. However, many prohibitions include far-reaching exceptions that could undermine their effectiveness. Civil society's active engagement will be essential to ensure harmful systems are explicitly recognised as prohibited.

Art. 5 will start applying in early 2025. The European Commission is currently developing guidelines on prohibitions. Civil society must sharpen the vague language of the Act and provide examples of existing systems that should be prohibited, together with legal reasoning.

Examples include:

Prohibition:	Exemptions:
Real-time remote biometric identification (RBI) systems (e.g., facial recognition cameras), but only **by law enforcement agencies and in public spaces**.	(1) The targeted search for victims of abduction, trafficking or missing persons; (2) the prevention of a substantial and imminent threat to life or physical safety or a genuine threat of a terrorist attack; or (3) localising or identifying a person suspected of committing so-called serious crimes (e.g., terrorism, human trafficking, murder, sexual exploitation of children). In those cases, RBI systems will be categorised as high-risk. Member States willing to use RBI systems **have to adopt national-level legislation authorising it.** Such systems have to undergo a fundamental rights impact assessment (FRIA) and each case of use requires a prior authorisation by a judge or an independent administrative authority. Both of these safeguards, however, can be delayed in a situation of urgency. Importantly, Member States can also introduce stricter rules on the national level, including a full ban for both real-time and "post" RBI. It is therefore crucial for civil society to engage on the national level to **prevent creating a blueprint for how to conduct mass biometric surveillance and to advocate for stronger safeguards.**

Prohibition:	Exemptions:
Systems which create or expand facial recognition databases by untargeted **scraping of facial images** from the internet or CCTV footage (e.g., systems like ClearviewAI).	
Systems which **infer emotions.**	Only applies to **workplace and education** (unless used for medical or safety reasons), leaving out migration and law enforcement where the risks of these pseudoscientific systems are arguably the gravest.
Systems which assign people based on their biometric data into categories inferring sensitive characteristics.	Does not include gender, gender identity, ethnicity (other than "race"), health status or disability. Does not apply to law enforcement when systems are used for "labelling or filtering" lawfully acquired biometric datasets. This means existing laws, especially data protection laws, remain highly relevant.
Predictive policing systems.	Limited to systems based on the **profiling of individuals** (as opposed to predictions about geographic areas) and does not apply to situations where the system **supports the assessment by a police officer** of the person's involvement in a criminal activity. The ban does not cover geographic crime prediction which is widely used in the EU and has been shown to reinforce existing racism and discrimination in policing.

All other relevant EU laws, e.g., data protection and anti-discrimination laws, continue to apply so civil society should continue utilising existing legislation to close the gaps left by the AI Act.

Of particular importance is the opportunity for Member States to authorise RBI (e.g., in Ireland or Sweden), or establish stricter rules or even a full ban (potentially in Germany or Austria).

The fact that some AI systems were not included in Article 5 does not automatically mean that they are allowed. All other relevant EU laws, e.g., data protection and anti-discrimination laws, continue to apply so civil society should continue utilising existing legislation to close the gaps left by the AI Act.

Recommendations for engagement around prohibited AI systems

High priority (2024)

	Timeline	Recommendation	Comments
RESEARCH	June-July 2024 & autumn 2024.	Crowdsource evidence of existing AI systems which would fall under each prohibition. Develop legal analysis to support this including in relation to data protection law, consumer protection law, non-discrimination law and international human rights law.	Evidence and analysis was submitted to the Commission by the EDRi AI Coalition in mid-June. Additional evidence could potentially be submitted by September or in public consultations of the guidelines in the autumn. Remaining gaps in evidence should be identified as well as approaches to building evidence around opaque systems, particularly in law enforcement. The Fundamental Rights Agency is currently conducting research on the use of RBI in the EU which civil society could try to feed into.
ADVOCACY	First draft of the guidelines for public consultations is expected in September 2024 but evidence should be provided to the Commission in June/July 2024.	Engage with AI Office Unit A2 in developing the guidelines on prohibitions to ensure that provisions are interpreted in a rights-based way and that exceptions are interpreted narrowly. (Note: while DG Connect is responsible for the guidelines, DG Just, as a directorate with expertise in fundamental rights and justice, is also feeding into the process.)	CSO input should be as concrete as possible, including examples of systems that should be prohibited, legal reasoning and specific language for amendments (see research above). Civil society must coordinate its input to prevent contradictions and ensure completeness, but the Commission often publishes quantitative data on the number of submissions it receives from different groups, so it could still be helpful for groups to submit individual responses, alongside a joint statement. Direct channels of communication with responsible individuals should be maintained alongside formal input in consultations.
ADVOCACY	June-December 2024.	Monitor and contribute to national-level legislation related to the use of RBI systems.	Member States who want to continue using RBI systems will have to have relevant legislation in place by the time prohibitions start to apply in early 2025. Based on widespread support for exceptions to Article 5 in the Council, we assume that most countries will develop such national legislation but only Ireland and Sweden have begun this process. Germany and Austria were both critical of exceptions to the RBI prohibition and civil society could push for stricter laws. In Germany, such efforts are already underway by, among others, AlgorithmWatch, Amnesty Germany and BEUC (and their German member, VZBV).
STRATEGIC LITIGATION	An action for annulment has to be brought within 2 months of the Act's publication (that is likely until September 2024).	Explore opportunities for a Member State or the EDPS to bring an action for annulment of Article 5 (especially regarding exceptions to RBI) before the CJEU as infringing on the Charter of Fundamental Rights.	This is sensitive as it requires a Member State or EU institution to act against an adopted EU law. Exploring this option requires knowledge of the political context and a good relationship with the government. Civil society could explore this in Austria, e.g., in partnership with the local digital rights organisation epicenter.works, who could be well-positioned to initiate such a conversation. The EDPS pushed for a full prohibition of RBI during the legislative process.

Medium and long-term priority (2025, 2026)

	Timeline	Recommendation	Comments
STRATEGIC LITIGATION	After Article 5 comes into force in early 2025.	Consider legal action against known systems being used, especially RBI systems, where countries have not adopted relevant legislation.	See more in section on strategic litigation.
CAMPAIGNING AND MOVEMENT BUILDING		Develop further strategy around campaigning for a full ban on RBI through the Reclaim Your Face campaign and mobilise supporters especially at national level around new laws authorising RBI.	Learn lessons from the Reclaim Your Face campaign and explore how the campaign could support national-level efforts related to biometric surveillance. Build alliances with academia to support legal and technical arguments. Gather evidence of harm and testimonies of people affected, possibly in collaboration with national human rights institutions and/or equality bodies.
ENGAGEMENT WITH AI PROVIDERS AND DEPLOYERS		Advocate with tech companies (large and small) for a voluntary moratorium on developing and selling exempted biometric systems to governments, and extend the AI Act protections beyond EU borders.	This would require a thorough mapping of the industry ecosystem as well as European companies which export systems that would be prohibited in the EU.

Classification of High-Risk Systems & Fundamental Rights Impact Assessments (FRIA): Article 6 and 27

Most AI Act requirements only apply to so-called "high-risk systems". Companies or institutions that put these on the EU market (providers), will have to produce technical documentation, create a risk management system and register their systems in a public EU database. All public sector and some private sector deployers of high-risk systems will have to conduct and publish a FRIA.

But there are exceptions to the transparency requirements for law enforcement and migration and a dangerous loophole where providers can self-assess their system as not posing a significant risk to health, safety or fundamental rights. In this case, neither the provider nor the deployer would be subject to obligations under the Act.

Civil society engagement will be essential in developing secondary legislation around these provisions to try to narrow these get-outs. Guidelines on how to categorise systems as high-risk, conditions for exemptions, and the template for FRIAs will all decide how effective safeguards can be.

The inclusion of mandatory FRIAs is an important preventative safeguard but the explicit requirements are relatively weak:

- Deployers of high-risk AI systems have to list potential impacts on fundamental rights, but there is no clear obligation to assess whether these impacts are acceptable, or to prevent them where possible (deployers only have to specify which measures will be taken once risks materialise).
- The requirement to consult external stakeholders, including civil society and people affected by AI, in the assessment process was also removed from the final text and instead is only mentioned in the recital. CSOs will therefore not have a direct, legally binding avenue to contribute to impact assessments.
- Law enforcement and migration authorities will not have to publish the results of FRIAs. Information will only be included in a non-public database, limiting public scrutiny.

Civil society will have to fight to make sure these do not become a tick box exercise and can nonetheless contribute to increased accountability of AI systems.

Recommendations for civil society engagement around classification of high-risk systems and FRIAs:

High priority (2024)

	Timeline	Recommendation	Comments
RESEARCH	End of 2024.	Crowdsource examples of existing AI systems which fall under various high-risk categories, as well as systems which should not be exempted under the Article 6 loophole.	Some organisations have already begun mapping high-risk systems (e.g., the European Partnership for Democracy engaged with the European Commission on high-risk AI systems in elections, and the Protect Not Surveil coalition led by Access Now is mapping such systems in the area of migration). Further coordination is needed.
RESEARCH	Conducted in 2024, so that a ready-to-use prototype can be presented to the AI Office in early 2025.	Develop a prototype template for a meaningful FRIA which addresses the identified gaps, based on experiences with existing frameworks (e.g., the Dutch Fundamental Rights and Algorithmic Impact Assessments).	This should ideally be done in collaboration with academic experts (e.g., authors of FRIA at Utrecht University, Prof. Alessandro Mantelero and Dr. Gianclaudio Malgieri). ECNL and Utrecht University are in discussions on a joint project. National human rights institutions should provide input and support (e.g., the Danish Institute for Human Rights have extensive expertise). Create alliances with smaller or local civil society groups, or people affected by AI systems to help shape the FRIA template.
ADVOCACY	Conducted in 2024, so that a ready-to-use prototype can be presented to the AI Office in early 2025.	Identify national governments and human rights institutions who can be allies in pushing for strong standards for FRIAs (e.g., the Netherlands, potentially Austria and Poland). Urge them to pledge support for the civil society template for FRIAs during Commission consultations.	This requires strong links to national governments. ECNL can play this role in the Netherlands but the plans and connections of other organisations should be mapped to determine if they can join these efforts.

Medium priority (2025)

	Timeline	Recommendation	Comments
ADVOCACY	Throughout 2025.	Use the research above to contribute to the European Commission (AI Office Unit A2) guidelines on high-risk AI systems, which will include a list of systems which can be and cannot be exempted from AI Act requirements.	For maximum impact, civil society should present joint submissions and gather support from other stakeholders. Building connections with the private sector remains challenging but we consider it worthwhile to map companies and investors who could be allies.
ADVOCACY		Coordinate and gather support from civil society and academia for the draft template for FRIA (see research above) and submit it as a joint civil society-academia proposal for the AI Office (Unit A2).	Explore alliances and support of the corporate sector.

Long-term priority (2026)

	Timeline	Recommendation	Comments
RESEARCH		Monitor the public EU database to identify AI systems which have been exempted from AI Act requirements under Article 6. Coordinate with CSOs in Member States to verify if similar systems were also exempted. Map discrepancies to provide as evidence to the European Commission, European AI Board and national competent authorities. Explore opportunities to complain against providers who unjustifiably exempted themselves.	This activity would require extensive monitoring and coordination. Often, it would also require collaboration with technical experts or investigative journalists, especially for AI systems intended to be used in law enforcement and migration which enjoy a lower level of transparency.
RESEARCH		Based on the EU database (see section on Transparency below), map high-risk AI systems to identify potential cases for litigation, campaigning or advocacy.	
ADVOCACY		Engage, in a coordinated manner, with national or EU-level public authorities which use high-risk AI systems, or with private companies covered by the obligation to conduct FRIAs (e.g., banks and insurance companies) to mainstream the civil society template for FRIAs and demand the setup of meaningful stakeholder engagement structures.	CSOs can raise issues and concerns, and advocate at national level for more voluntary types of accountability and disclosure, including in connection with the newly adopted Corporate Sustainability Due Diligence Directive which creates obligations for tech companies to assess human rights impacts throughout their supply chain.

National security exemption: Article 2

The AI Act includes a blanket exemption from its requirements for AI systems developed or used exclusively for national security purposes. There is no clear definition of what constitutes national security, leading to concerns this exemption will be used as a pretext to use harmful AI systems, even those that are otherwise prohibited, without any transparency or accountability. Civil society's work will be crucial to challenge the legal basis of the exemption, to collect and expose evidence of the use of AI for national security, and to continue advocating with national governments as well as the private sector for moratoriums, bans and necessary fundamental rights safeguards.

The AI Act excludes from its scope all AI systems that are either created and deployed from the very beginning for national security purposes, or that are eventually used for national security purposes, regardless of their initial purpose. It is argued that this exemption is justified by the fact that national security is an exclusive responsibility of EU Member States. However, this is not in line with the established jurisprudence of the CJEU that any exceptions must be considered on a case-by-case basis, in line with the Charter on Fundamental Rights. Moreover, there is no clear distinction between national security and law enforcement activities. While the former are exempt, the latter are covered (albeit with extensive caveats) by the AI Act.

Recommendations for civil society engagement around national security exemption:

High priority (2024)

	Timeline	Recommendation	Comments
STRATEGIC LITIGATION	June-July 2024 Note: an action for annulment has to be brought within 2 months of the Act's publication.	Explore options for a Member State to bring an action for the annulment of Article 2 before the CJEU as infringing on the Charter of Fundamental Rights.	Similarly to comments in the prohibitions section (Article 5) this is a highly time-sensitive and political issue which requires the identification of national-level allies. This might be a lost battle, as no single country was firmly opposed to the exemption in the negotiations.

Medium and long-term (2025 and beyond)

	Timeline	Recommendation	Comments
RESEARCH	Throughout 2025.	Map the procurement and/or use of AI systems exclusively for national security purposes in their EU Member States. After the AI Act comes into effect in 2026, map which AI systems are put into service or placed on the market by their providers for dual use, including potential use for national security purposes.	Due to the secrecy surrounding the national security uses of AI, this will require collaboration with investigative journalists and strategising around tactics for obtaining information. It is also an open question as to which countries should be prioritised.
ADVOCACY	2025 & beyond.	Develop strategies for advocacy with national governments to strengthen fundamental rights protections in national security, (e.g., by adopting national laws which apply other AI Act requirements to national security).	
STRATEGIC LITIGATION		Explore options for litigation in preselected Member States with the view for the court to ask preliminary questions to the CJEU in order to clarify the scope of the exemption.	

Transparency: Articles 26, 49, 50, 71 and Annex VIII

The AI Act requires all providers, as well as public sector deployers, of high-risk AI systems to register in a public database maintained by the European Commission. This register should include some technical information as well as the results of FRIAs. This measure gives civil society important tools to investigate, for example, systems used by public authorities to allocate benefits, or by schools to assess students, although there are again loopholes for law enforcement and migration.

Additionally, the AI Act requires deployers of high-risk systems to inform people that they are subject to decision-making with the use of AI. However, Art. 13 of the Law Enforcement Directive applies, which means that Member States can restrict the right to be informed in most cases so that it is very likely that no information will be shared with people affected by (for instance) predictive policing or risk assessment systems. People will also have to be informed when they interact with chatbots and see content generated by AI. But there is an exemption for law enforcement authorities that use chatbots, generative AI (including deep fakes), emotion recognition or biometric categorisation as part of investigations.

As well as suffering from these exemptions, many of the requirements under these provisions are vague. Civil society has an opportunity to influence how transparency will look in practice and ensure these provisions are meaningfully implemented.

The EU database will include information from providers about high-risk AI systems that are available on the EU market, including:

- The identity and contact details of the provider.
- The description of the intended purpose of the AI system.
- A basic description of the input data used by the system and its operating logic.
- In which Member States the system has been made available and put into use.
- Instructions for use which include more detailed technical information about the system, including the system's performance metrics and design features, as well as identified risks.

It also includes information from deployers of high-risk AI systems that are used in the EU, but only in the public sector, including:

- The identity and contact details of the deployer.
- The intended purpose of the system.
- The summary of the findings of FRIAs and the data protection impact assessment.
- The link to the entry in the database made by the provider who sells this system.

And it includes information about AI systems which have been exempted from fulfilling obligations:

- The intended purpose of the AI system.
- The conditions based on which the AI system is not considered to be high-risk, together with a summary of the reasoning.
- In which Member States the system has been made available or put into use.

The European Commission is in charge of designing the database and is required to consult with relevant experts and stakeholders. This is an opening for civil society to ensure that the database contains useful information. Once established, it can be used to identify potentially harmful systems, contact their providers or deployers, and assess the results of FRIAs.

Information from both providers and deployers of systems used in law enforcement and migration will only be available to the Commission and national authorities, not the public. They also will not include instructions for use or a description of the logic of the systems, making it very difficult for supervisory authorities to understand how the system works. Deployers will have to register the findings of FRIAs but not data protection impact assessments, nor include a link to the provider's entry in the database. Real-world testing of law enforcement and migration systems does not have to be registered at all.

These are sweeping loopholes which create total opacity for how AI is actually used in law enforcement and migration. This severely impacts civil society's capacity to investigate these systems and keep them accountable, and does not improve the status quo. Civil society will have to continue investigating these harmful uses of AI using existing methods, e.g., through investigations, freedom of information requests and procurement records.

The European Commission is in charge of designing the database and is required to consult with relevant experts and stakeholders. This is an opening for civil society to ensure that the database contains useful information. Once established, it can be used to identify potentially harmful systems, contact their providers or deployers, and assess the results of FRIAs.

No guidelines are planned to provide more details about the obligation on deployers of high-risk AI systems to inform individuals if they are subject to the use of the system. The Commission will, however, issue guidelines on the practical application of Article 50 to inform people of the use of generative AI, deep fakes, chatbots, emotion recognition and biometric categorisation, and is explicitly required to involve external stakeholders in the process.

Recommendations for civil society engagement around transparency:

Medium priority (2025)

	Timeline	Recommendation	Comments
RESEARCH	First half of 2025.	Develop detailed recommendations for information that should be included in the EU database as well as for information to be provided to people affected by AI systems. This can also include mock-ups or prototypes.	This research may require technical and design expertise. The latter will be relevant for developing potential mock-ups or prototypes of the EU database or individual information notices, especially for outputs of generative AI or chatbot systems. Technical expertise might be necessary to translate some of the requirements from Annex VIII into concrete and actionable types of information related to the development or functioning of the AI system that should be made public. Some work on this has already been done in the past by, among others, AlgorithmWatch and Panoptykon Foundation.
ADVOCACY		Influence the design of the EU database on what specific information should be included for each of the categories listed in Annex VIII.	Civil society needs to identify and confirm which unit of the European Commission/AI Office will be responsible for the set up and maintenance of the EU database. There might also be opportunities to contribute on the national level because Art. 71 of the AI Act explicitly says that the Commission should collaborate with Member States when developing the database.
ADVOCACY		Contribute to guidelines on the practical application of transparency requirements from Article 50. Advocate for the guidelines to also include requirements for information to be provided to people affected by high-risk AI systems, based on Article 26.	
ADVOCACY		Demand access for civil society for the development of the code of practice on generative AI.	More work is needed to identify relevant actors in the development of the code of practice on the labelling of outputs of generative AI.

Long term (2026 and beyond)

	Timeline	Recommendation	Comments
ADVOCACY		Advocate with specific deployers of high-risk AI systems for best practices on informing people about being subjected to AI.	If efforts for implementation at EU level are not successful, civil society should continue advocating for best practices and voluntary commitments by private and public sector providers and deployers.
STRATEGIC LITIGATION		Explore options for utilising existing laws and tools to cast more light on AI systems used in the area of law enforcement and migration.	
CAMPAIGNING		Continue exposing harmful uses of AI in law enforcement and migration, and campaign around increasing transparency, (e.g., exploring options for amending the AI Act in this regard).	

Redress and individual rights: Articles 85 and 86

The AI Act, as a piece of a "product safety" legislation, did not originally include any rights for people affected by AI. Thanks to civil society advocacy, the AI Act introduces the right for anyone to lodge a complaint with a market surveillance authority, the possibility for consumers and consumer organisations to use collective redress mechanisms, and the right to an explanation of individual decision-making. Civil society should test these mechanisms, although their limitations also underline the importance of using existing laws, especially the GDPR, for keeping AI systems accountable.

Civil society should test these mechanisms, although their limitations also underline the importance of using existing laws, especially the GDPR, for keeping AI systems accountable.

Unlike the GDPR, the AI Act does not create an individual right to complain. Rather, it gives anyone the right to flag infringements to the market surveillance authority, even if they are not directly affected. Such complaints should be taken into account for conducting market surveillance activities, but the authority does not have to issue a specific decision on them. When it comes to collective redress, it will be possible to use representative action, in line with the collective redress directive, to seek redress for AI Act violations, but only where it affects "consumers" and not people's broader lives as citizens. This means it will apply mostly to systems used for credit scoring, insurance premiums, and general-purpose/generative AI when it is used in the private sector. Additionally, the right to explanation applies to any person subject to a decision taken based on the output from a high-risk AI system which "produces legal effects or similarly significantly affects that person". This complements the existing right to an explanation under the GDPR and appears to extend it beyond solely automated decisions to those where AI has supported a human decision. There is still, however, potential for the EU and Member States to limit this right, most likely in law enforcement and migration.

Recommendations for civil society engagement around redress and individual rights:

High priority (2024)

	Timeline	Recommendation	Comments
COORDINATION		Establish a coordination group for organisations interested in exploring redress options and strategising around strategic litigation and possible cases to bring once the AI Act enters into effect, especially for prohibitions which will apply from early 2025.	
RESEARCH	Preparation to bring first case in 2025, after prohibitions come into effect.	Begin mapping opportunities for strategic use of new mechanisms, both in the public sector and in the private sector (in partnership with consumer organisations) and identify a strong first case.	Note the potential challenge: prohibitions become applicable in early 2025 (probably February) but the deadline for Member States to actually set up market surveillance authorities who could receive complaints is in June 2025. This can create a temporary vacuum in terms of accountability and leaves an open question about redress options should civil society identify an AI system that is being used, despite fulfilling the conditions to be prohibited.

Medium to long-term priority (2025-2026)

	Timeline	Recommendation	Comments
ADVOCACY		Advocate at EU level with the EDPS, and with national governments (or specific market surveillance authorities) for the procedure of handling complaints to include a requirement for the authority to provide feedback to complainants about whether and how their complaint was taken into account.	National human rights institutions, equality bodies and other agencies could potentially serve as allies.
ADVOCACY		Engage with governments which propose national legislation which would exempt law enforcement and migration authorities from having to provide the right to explanation.	National-level CSOs need to monitor any attempts to limit the scope of the right to explanation by exempting law enforcement and migration authorities.

Accountability of generative and general-purpose AI (GPAI): Articles 51 to 56

The AI Act creates dedicated obligations for providers of GPAI models, which includes generative AI. This includes a policy to comply with copyright rules and publishing a summary of what content they use to train their models. Additionally, the European Commission will designate some GPAI models as presenting "systemic risks" which face additional obligations. In addition, as mentioned in the section on transparency, the outputs of generative AI systems must be marked and detectable as artificially generated. Given the high public profile of GPAI, particularly ChatGPT, the ability of the AI Act to have an impact on these systems will be a key test of its effectiveness. Civil society should influence the code of practice that will make these obligations concrete and put pressure on the Commission regarding which GPAI models will be designated as posing systemic risk.

Obligations for providers of all GPAI models include:

- Maintaining technical documentation and providing it to the AI Office and national competent authorities upon request.
- Making available information and documentation to providers of AI systems who intend to integrate the GPAI model into their AI systems.
- Putting in place a policy to comply with EU law on copyright and related rights.
- Making publicly available a summary about the content used for training of the GPAI model.

GPAI models that are released under a free and open-source licence that allows for the access, usage, modification, and distribution of the model, and whose parameters are made publicly available are exempt from these obligations if they also do not pose a systemic risk.

Additional obligations for providers of GPAI models with systemic risks:

- Identifying and mitigating systemic risks.
- Documenting and reporting to the AI Office and to national competent authorities about serious incidents and possible corrective measures to address them.
- Ensuring an adequate level of cybersecurity protection."

The enforcement of all these obligations sits with the Commission via the AI Office. Until a harmonised standard is finalised and published, providers can rely on codes of practice to demonstrate compliance. The AI Act recommends that these codes of practice should establish a risk taxonomy of the type and nature of the systemic risks at EU level – including their sources – and provide specific risk assessment and mitigation measures. The Commission may approve a code of practice and give it general validity within the EU.

Recommendations for civil society engagement around GPAI:

High priority (2024)

	Timeline	Recommendation	Comments
RESEARCH	Completed by the end of 2024.	Develop recommendations for how the notion of systemic risk should be interpreted under the AI Act and map existing GPAI models which should be designated as posing systemic risks.	There is a need for coordination between groups working on the DSA, which also includes the notion of systemic risks, (e.g., AlgorithmWatch, the Global Network Initiative, and groups working on the AI Act). Currently most of these groups operate in silos but mutual learning will be important.
ADVOCACY		Engage the AI Office on the development of the code of practice to ensure that civil society participates.	
ADVOCACY		Develop and present a "mirror" code of practice, grounded in fundamental rights and societal impacts of GPAI.	A group of organisations including SaferAI, Future Society, CDT, Pour Demain and Future of Life Institude developed a collaborative contribution to the GPAI Code of Practice. However, it should be consulted with a broader range of CSOs, especially when it comes to the part related to the assessment of risks which is currently not grounded in fundamental rights.

Medium priority (2025)

	Timeline	Recommendation	Comments
ADVOCACY	First half of 2025.	Engage with the scientific panel of independent experts to establish a channel of communication for bringing the evidence needed to raise alerts on GPAI models presenting systemic risks.	
ADVOCACY		Monitor and contribute to the designation of GPAI models posing systemic risk with the AI Office. Where needed, mobilise people to support advocacy.	

Migration

The AI Act persistently creates loopholes and exemptions around migration.

As we have highlighted throughout our analysis, the AI Act persistently creates loopholes and exemptions around migration. According to the Protect Not Surveil coalition, it will fail to prevent harm or provide protection for people on the move. We therefore wish to emphasise the need for a specific effort by civil society to challenge this across all aspects of the implementation of the AI Act, particularly in light of the increased presence of the far-right in the new European Parliament.

Recommendations for civil society engagement around migration:

High priority (2024)

	Timeline	Recommendation	Comments
RESEARCH	Prohibitions urgently High-risk AI systems until the end of 2024	Crowdsource and contribute migration-specific examples of existing AI systems that should be included in prohibited AI practices. Contribute them to civil society input for the Commission. Map and share knowledge about the use of high-risk AI in a migration context, at the EU and national levels.	These recommendations are based on the planned strategy of the Protect Not Surveil coalition. To expand on these recommendations, consultation with the coalition and a needs and gaps assessment is needed for assessing capacities and the prioritisation of support.
COORDINATION	2024	Continue coalition building for the Protect Not Surveil campaign, including a broad array of CSOs, and ensuring that the coalition includes and supports the work of grassroot movements, especially migrant-led groups.	
ADVOCACY		Develop an advocacy strategy linking AI Act implementation with other political and legislative developments in the area of migration, policing and surveillance.	

Medium priority (2025)

	Timeline	Recommendation	Comments
RESEARCH		Map and conduct exchange about actors and the work being done on alternative visions of the migration sphere, without surveillance technology.	
ADVOCACY		Feed migration-related expertise and perspectives into relevant implementation processes (e.g., guidelines for high-risk AI systems with AI Office Unit A2).	

Long-term priority (2026 and beyond)

	Timeline	Recommendation	Comments
CAMPAIGNING AND MOVEMENT BUILDING		Build and mainstream positive visions and proactive demands in policy processes.	External support and capacities in visioning, advocacy in restrictive contexts, alternative approaches etc... could be necessary. Civil society should identify gaps in existing capacities.

Influencing technical standards

In practice, much of the implementation of the AI Act requirements will take place through the adoption of technical standards. AI providers that apply the technical standards approved by the European Commission (so-called harmonised standards) are presumed to be in compliance with the relevant requirements of the AI Act. The burden of proof is then on the market surveillance authority to show that they have violated them. However, the complexity of fundamental rights is not easily translated into technical specifications, and standards development bodies, namely the CEN/CENELEC, lack necessary expertise in this area. Civil society should try to use the available, albeit imperfect, pathways to engage in the standardisation process. Once the standards are adopted, civil society should review them and, if needed, advocate with the European Commission not to accept them.

The European Commission's standardisation request was issued in 2023 and obliges standardisation bodies to facilitate an appropriate representation and effective participation of relevant stakeholders in the development of the standards mandated to support the AI Act. The standard-setting body CEN/CENELEC established a Joint Technical Committee 21 (JTC-21), which is responsible for developing standards for high-risk AI systems as categorised within the AI Act. There is limited civil society representation on the JTC-21 working groups (ANEC, which represents consumers; ETUC, the European Trade Union Confederation which represents employees and workers; and ECOS, the Environmental Coalition on Standards). Most experts are employed by companies, acting as delegates of the national members of CEN/CENELEC.

List of issues to be standardised:[1]

- Risk management systems (including assessment and mitigation of risks to fundamental rights).
- Governance and quality of datasets used to build AI systems (including the elimination of bias).
- Record keeping through logging capabilities.
- Transparency and information provisions towards deployers.
- Human oversight.
- Accuracy specifications.
- Robustness specifications.
- Cybersecurity specifications.
- Quality management systems, including post-market monitoring processes.
- Conformity assessment.

All of these issues have implications for fundamental rights but the most important are likely to be risk management systems, data quality governance, human oversight and conformity assessments

All of these issues have implications for fundamental rights but the most important are likely to be risk management systems, data quality governance, human oversight and conformity assessments, to be discussed from 2024 onward.

CSOs face obstacles to influencing standards processes, including lack of time and resources, lack of technical expertise and the dominance of big tech representatives. A dedicated Task Group (TG) on Inclusiveness was set up within JTC 21 "to reflect on ways to reach out to relevant stakeholders" and has set up a newsletter – but this is not enough to ensure meaningful inclusion. Additionally, the working group of the JTC21 focused on "Foundational and Societal Concerns" (WG4) has established a new workstream related to fundamental rights. This will prepare a Technical Report (TR) to "explore technical and organisational measures to safeguard fundamental rights", including a gap analysis in existing standards from a fundamental rights perspective to identify any necessary measures to help ensure proper inclusion of fundamental rights considerations across all technical standards being developed by JTC21. ETUC (the trade unions representative) has been appointed as the coordinator of this workstream and intends to use this platform to translate high level fundamental rights input into technical requirements that can be used effectively within standardisation.

CSOs face obstacles to influencing standards processes, including lack of time and resources, lack of technical expertise and the dominance of big tech representatives.

1 Note that updates to the work programme are published here.

Given these challenges, we recognise that civil society engagement in standardisation processes may be limited to those with the necessary capacity, expertise and networks. It is important, however, that these representatives can translate wider civil society objectives into the process.

Recommendations for civil society engagement in technical standards:

Recommendation	Comments
High priority (2024)	
Coordination CSOs interested in the standardisation process should coordinate to develop clear areas of focus and objectives for specific standardisation deliverables, taking into account existing avenues for input and capacity.	An informal group has been set up previously by ECNL, in collaboration with Access Now, BEUC, Article 19, Amnesty Tech, European Disability Forum and a few other organisations. Organisations willing to join coordination should contact ECNL.
High and medium priority (2024 and 2025)	
Contribution to the standardisation process	CSOs who are not members of CEN/CENELEC would need to utilise existing members (including social partners ETUC, ANEC, Equinet, CEN members and CENELEC members) to channel their input quickly and request additional consultation and sessions dedicated to fundamental rights. In addition, CSOs can approach their national level (friendly) standard bodies who are members of CEN to provide input, where possible. We suggest five priorities for engagement based on our assessment of urgency and feasibility, with focus on Priority 1 as the most feasible.
Priority 1: Provide input toWG4 workstream on fundamental rights How? Provide comments through ETUC and by directly contacting TG Inclusiveness coordinated by ETUC at TG_Inclusiveness@etuc.org When? Urgent in 2024.	We have identified this workstream as the most promising for providing civil society input, given that the main goal of this process is to comprehensively monitor standardisation deliverables through the lens of fundamental rights, identify gaps and directly contribute to key deliverables. As such, this workstream can serve as a "one-stop-shop" for civil society to contribute comments regarding fundamental rights. In addition, ETUC, who is leading this workstream, has offered to provide avenues to keep CSOs informed about developments, and facilitate input.

Recommendation	Comments
High and medium priority (2024 and 2025)	
Priority 2: Provide input into key standardisation deliverables When? Continuous, based on timeframes for specific deliverables.	As an alternative to providing contributions through WG4's workstream on fundamental rights, civil society can also contribute to specific deliverables directly through working groups dedicated to them. However, this would require a closer monitoring of specific working groups and connection to their existing members, including members of national delegations. At the same time, this avenue might be more effective for CSOs who have technical expertise on issues such as bias or cybersecurity or for national-level CSOs with good connections to national delegations to CEN/CENELEC.
Priority 4: Assess fundamental rights considerations once standards are finalised How? Engagement with the European Commission. When? Estimated second half of 2025, first half of 2026.	After all standardisation deliverables are finalised, they have to be approved by the European Commission and published in the official EU journal to become so-called "harmonised standards". This results in the presumption of conformity for AI providers. Civil society could engage in assessing the extent to which the developed standards are in line with fundamental rights. This should be possible thanks to the recent CJEU ruling which confirmed that all harmonised standards have to be made publicly available free of charge (even though it's not clear whether that applies to draft harmonised standards before they're approved). In any case, a coordinated effort by CSOs should target the European Commission to allow CSO interventions and assessment before approval. As the advocacy target in this context would be the European Commission, as opposed to CEN/CENELEC, this activity might be more accessible for CSOs who have not engaged with JTC21. This engagement requires human rights expertise and cooperation with technical experts in AI as well as auditing/impact assessment experts.

Recommendation	Comments
Long-term priority (2026 and beyond)	
Priority 5: Advocate for the development of common specifications, if necessary When? 2026.	In case the Commission concludes that the harmonised standard does not sufficiently take into account fundamental rights concerns, it can develop so-called common specifications whose aim would be to complement standards. As common specifications are developed by the Commission, this could be a more accessible pathway for civil society to address the gaps related to fundamental rights.

Pathways to strategic litigation

Legal experts, litigation practitioners, people affected by AI systems and CSOs need to explore potential litigation topics together.

As noted throughout the analysis of the different provisions of the AI Act above, strategic litigation is an important tool in both addressing the limitations and loopholes within the Act itself, and in achieving accountability in practice through ensuring that its requirements are enforced. Due to the very limited avenues for redress in the Act (see section above) litigation will have to go beyond the Act and draw on other existing EU fundamental rights legislation including GDPR, the future AI Liability Directive, and national level regulation. Legal experts, litigation practitioners, people affected by AI systems and CSOs need to explore potential litigation topics together. These could include:

- Challenging the blanket national security exemption (Article 2) before the CJEU (time limited and politically sensitive).
- Addressing law enforcement and migration loopholes throughout the AI Act before national courts, the EU Ombudsman or CJEU.
- Challenging national-level legislation authorising RBI systems.
- Litigation against a provider/deployer of an AI system that should fall into the scope of prohibitions.
- Litigation related to the lack of compliance of a specific high-risk AI system.
- Challenging an exemption of an AI system from AI Act requirements based on Art. 6(3).
- Lack of designation of a GPAI model posing systemic risk or inadequate transparency or risk assessment.

Recommendations for the development of strategic litigation by civil society

Recommendation	Comments
High priority (2024)	
Coordination: • Create a pre-litigation coordination group of interested and committed CSOs to work on mapping litigation areas and pathways in detail. • Involve academics with experience in supporting litigation, as well as pro-bono litigators willing to provide input into the initial mapping. • Organise and facilitate a series of pre-litigation mapping workshops for the group above (or broader) with the aim of identifying priorities and initial legal pathways for each of the priorities (see proposed areas listed above).	A coordination group needs to be set up. ECNL is interested in co-leading it to discuss and map potential legal pathways for diverse issues.
High and medium priority (2024 and 2025)	
Research: • Consolidate pre-litigation mapping and strategise on legal pathways for each of the priorities/issues (see proposed areas listed above). • Match additional stakeholders (e.g., legal practitioners, academics) interested and willing to contribute to specific issues. • In subsequent workshops, each specific priority area will need the development of a legal file with legal experts and litigation practitioners, addressing specific pre-litigation issues, e.g., legal standing, forum/jurisdiction, cross-border law application, harms identification, potential applicants, most promising avenues for achieving the goals. • Develop concrete pre-litigation files for priority issues. • Explore options for campaigning around litigation.	Ideally, different sub-groups should emerge based on issues to pursue that are deemed promising for legal challenges. For each specific pre-litigation file, the sub-group will develop concrete action steps, actors needed and cost projections for fundraising.
Long-term priority (2026 and beyond)	
• Launch legal challenges and sustain litigation. • Launch campaigns supporting litigation.	

Lessons from the Digital Services Act (DSA)

The ongoing civil society involvement in the implementation and enforcement of another recent EU cornerstone regulation, the DSA, holds important lessons for the success of the AI Act. The overall assessment of CSO engagement in the implementation and enforcement of the DSA so far is largely positive. Civil society enjoys a high level of access to the European Commission's DSA Enforcement Team and Digital Services Coordinators (DSCs) at the national level. Civil society has positioned itself as an important interlocutor with a wealth of expertise and research that can support the Commission's enforcement work. A number of civil society recommendations have been embedded into open investigations or (draft) delegated acts. CSOs indicated[2] that the following factors enabled engagement:

- Successful coordination between CSOs presenting a unified voice.
- Alignment of high-level goals between CSOs, policymakers and regulators, which facilitates better relationships.
- The unprecedented level of openness on the side of the Commission, possibly enabled by the sense of urgency linked to the ongoing violations by online platforms.
- The novel nature of the DSA, where CSOs managed to establish themselves as providing expertise crucial for the success of the law.

At the same time, CSOs highlighted several challenges which hold important lessons for both the DSA and the AI Act implementation. Below we present key learnings, together with recommendations in the context of AI Act implementation, across three topics:

- Civil society coordination and access to funding.
- Gaps in expertise and national-level involvement.
- Engagement with the European Commission.

2 Methodology: Online survey distributed with the DSA Civil Society Coordination Group (facilitated by CDT) and the EDRi Platform Working Group. Online interviews with: Eliška Pírková, Senior Policy Analyst and Global Freedom of Expression Lead, Access Now; Asha Allen, Director of Europe Office, CDT Europe; Jan Penfrat, Senior Policy Advisor, EDRi; Julian Jaursch, Project Director "Strengthening the Digital Public Sphere and Platform Regulation", Stiftung Neue Verantwortung. ECNL's own observations as an organisation involved in both the DSA and AI Act implementation.

Coordination and access to funding

CSO coordination, which started during the legislative process and has continued over implementation, has been very successful. The leading coordination groups include the DSA Civil Society Coordination Group facilitated by CDT Europe, the platforms working group within EDRi, and the Recommender Systems Task Force facilitated by Panoptykon. These have helped with sharing intelligence and updates, ensuring the distribution of CSO resources across different topics and issues, and identifying a joint high-level advocacy priority (formalised, systemic engagement with civil society).

However, coordination within the DSA Civil Society Coordination Group becomes more challenging as new groups seek to join the coalition. Some CSOs argue that for effective advocacy towards EU institutions, coalitions should be relatively small to enable the alignment of positions and joint meetings with the Commission. According to some, the strength of the group comes from the fact that there is a core group of CSOs, mostly Brussels-based, who set the pace for the larger coalition, provide updates and coordinate activities focused on specific topics.

There are also questions of due diligence towards candidates who have not been recommended by any of the existing members, particularly organisations which include corporate members or represent the views of companies. It was also emphasised that it's important to devote time to building trust among coalition members for the coordination to work effectively. Coordination, which began organically, is expanding and becoming more time-consuming (e.g., regular online meetings and roundtable series). This raises the question of funding, as not all CSOs have funds to cover the time and resources needed to coordinate with others.

Many CSOs noted that access to funding beyond advocacy and campaigns in the legislative process is a challenge. There is a strong need expressed by CSOs for funders to support work related to implementation and enforcement. In a way, civil society contributions have so far increased the Commission's expectations for civil society-led research and legal analysis, all of which are very resource-intensive. According to many CSOs, private funding is the only option, as European Commission funds come with burdensome requirements and are insufficient.

In addition, some CSOs, particularly from Central, Eastern and Southern Europe, are concerned about the lack of funding for national-level work, e.g., for CSOs to engage with Digital Services Coordinators or to act as trusted flaggers.

Effective coordination between different groups of CSOs is crucial for successful implementation and enforcement.

Lessons for the AI Act:

- Effective coordination between different groups of CSOs is crucial for successful implementation and enforcement. CSOs should newly establish or extend an existing coordination group to include thematic sub-working groups with specific mandates (e.g., litigation or a certain topic), and share information to make sure everyone benefits from lessons learned and avoids duplication. The EDRi AI coalition could be well-placed to serve this role as an already well-established coordination group.
- In the context of the AI Act, there is concern about longtermist/effective altruism groups joining civil society coalitions, and about civil society legitimising such groups. These groups receive a lot of visibility and influence with institutions, but there is concern that they shift policymakers' attention away from the existing, real-life harms of AI, towards hypothetical "existential threats" in the distant future. CSOs should clarify their concerns and approach towards collaborating or entering coalitions with such organisations.

What funders can do

Support implementation and enforcement work, especially resource-intensive preparatory activities (technical investigations, legal analyses and litigation pre-research).

Channel dedicated funds for coordination, both by supporting the coordinating organisation(s) and coalition members, especially on the national level (e.g., through sub-grants by the coalition leaders).

Support financially or directly organise periodical in-person convenings, on the EU and national level, that would create the space for CSOs to build closer relationships, and strategise concrete steps together on key topics of interest.

Gaps in expertise and national-level involvement

Some CSOs have struggled to find their place in the DSA implementation and enforcement process, as they do not have many of the specific skills that these processes require (e.g., research or technical investigations). There is a need for more effective mechanisms to fill these gaps. While some CSOs have established ad-hoc groups of data scientists, engineers and designers ready to lend their expertise pro bono or at a small fee, they are concerned that such forms of collaboration are not effective in the long run.

There is a strong conviction that CSO engagement is needed both at EU and Member State level, due to shared enforcement responsibilities. At the same time, while coordination on EU-level implementation and enforcement is very effective, few organisations are involved in national-level work. National context is crucial, especially for issues like election disinformation or appointing trusted flaggers. The absence of capacity can lead to missed opportunities for identifying or preventing issues (e.g., election disinformation in Slovakia). There is a need for improved exchange of information and coordination among the national implementations of the DSA, to understand good practices adopted in different countries which could be transplanted elsewhere.

Lessons for the AI Act:

- Given the breadth of secondary legislation in the AI Act and the focus on consulting technical stakeholders, civil society, supported by funders, should map all secondary legislation of the AI Act and assess which should be prioritised. Note that this paper aims to fulfil this task in part 3 and Annex I but more discussion is needed with a broad range of CSOs to validate ECNL's assessment, map existing activities and identify needs and gaps.
- Based on this mapping, CSOs should strategise concrete action steps for specific topics and, where necessary, establish dedicated working groups.
- Access to technical expertise is likely going to be even more relevant in the context of the AI Act, which relies even more heavily than the DSA on technical standards.

Access to technical expertise is likely going to be even more relevant in the context of the AI Act, which relies even more heavily than the DSA on technical standards.

What funders can do

Facilitate collaborations with external technical experts, for example by establishing a network of public interest technologists and "matching" experts with (groups of) CSOs on a well-defined task (e.g., based on their joint application). This approach would promote cooperation in civil society on emerging topics (instead of competing for rare expertise), and partially remove the burden of managing external relationships.

Support the work of national-level CSOs, especially in countries where a high number of high-risk AI systems are being developed or used. Additional research could be commissioned to establish national-level priorities (e.g., which countries or issues to focus on) and consult civil society about their needs.

Engagement with the European Commission

The European Commission has been very open to engaging with civil society in the DSA implementation and enforcement process. For example, the Commission has committed to hold regular roundtables with civil society and established dedicated contact points for CSOs. At the same time, much of the engagement with the Commission is based on the personal relationships some CSOs (mostly active in Brussels) have with members of the DSA Enforcement Team. Many CSOs, especially at the national level, do not enjoy the same level of access, unless others help them leverage their expertise, which many assess as unsustainable in the long run. While informal relationships with DSA Enforcement Team members are important for gaining information and providing feedback, the question arises as to how the Commission selects who it will engage with, and whether it can ensure that the relevant expertise of smaller groups, perhaps less visible in Brussels, can be taken into account.

Commission attempts at organising more structured consultations have been widely judged as unsatisfactory – and even a misuse of civil society time and capacity – which raises concerns about superficial stakeholder engagement models that the Commission might replicate in the future.

CSOs have also voiced concerns about the risk of blurring the boundaries between the Commission as a regulator and CSOs as watchdogs. For example, civil society has to maintain independence in order to be able to publicly criticise the Commission. CSOs should be able to indicate where their resources can be put to the best use without the fear of losing access to the Commission.

Moreover, industry is very uncomfortable with CSOs talking directly to regulators and is striving to limit this by pushing for direct engagement with the Commission or for multi-stakeholder processes, in which CSOs' voices can be easily outnumbered or silenced by industry representatives.

Lessons for the AI Act:

In the AI Act, the broad policy goals of civil society and the regulator are not as aligned as they are under the DSA. Sometimes they are even at odds, especially when it comes to law enforcement, national security or migration issues.

- In the AI Act, the broad policy goals of civil society and the regulator are not as aligned as they are under the DSA. Sometimes they are even at odds, especially when it comes to law enforcement, national security or migration issues. We can therefore anticipate that the same level of openness and engagement with the Commission might be more difficult. Civil society should therefore jointly focus on advocating for structured and long-term engagement exclusively with civil society stakeholders rather than only through multistakeholder bodies like the advisory forum. Strategically and early on, CSOs should put this issue on the table for every new body established by the AI Act, or existing bodies designated for implementation, to ensure a coordinated and concerted effort to put pressure on relevant bodies until they allow for structured engagement.
- Civil society should aim to identify industry champions that could act as allies. Recognising the difficulty in the context of AI, collaborations can be explored on a case-by-case basis (e.g., some companies might be ready to support CSOs on issues like prohibitions or law enforcement uses of AI but not others).
- CSOs active on the EU level should strive to leverage the expertise of other CSOs, especially groups representing marginalised communities. At the same time, CSOs should urge the Commission to ensure that there are systemic outreach processes in place within the Commission. CSOs could explore complaints to the EU Ombudsman if this is not the case. Alternative approaches remain an open question that should be strategically addressed in the broader CSO community, as this does not only apply to digital policies.

- On the national level, civil society should also push for establishing systemic engagement with civil society. For example, the advisory council established at the German Digital Services Coordinator (an informal multistakeholder body) can serve as an inspiration and best practice.

What funders can do

Support civil society efforts to establish meaningful and sustainable pathways for civil society engagement with the European Commission and relevant national authorities.

Convene, or support convenings, aimed at strategising pathways for engagement or potential complaints to the EU Ombudsman.

Establish and facilitate connections with the business sector (e.g., by conducting or supporting ecosystem mappings aimed at identifying responsible AI providers).

Conclusion

Above all, the response must centre the people most affected by AI and ensure their interests are represented throughout.

Civil society has punched well above its weight in the development of the AI Act. While the law remains imperfect, it goes some way to establishing accountability over AI technologies and challenging the harmful impacts of AI on people and society. But civil society's victories will remain symbolic if public interest advocates do not see the AI Act through to implementation and enforcement. Only then will the public benefit of AI regulation be felt.

This will require sustained effort and engagement by civil society – both those involved in the AI Act development and new actors that can introduce skills, such as technical research and strategic litigation. Above all, the response must centre the people most affected by AI and ensure their interests are represented throughout.

None of this work is possible unless individuals and organisations have the resources to conduct it. Public funding remains limited and burdensome while corporate funding represents a conflict of interest. There is, therefore, a responsibility on philanthropy to support this work over the next two years and beyond.

We encourage funders to draw on the insights of this research as they plan their grantmaking and continue to engage with civil society to understand where their investments can be most effective. The European AI & Society Fund will continue to work with its funding partners and others across the philanthropic field to support and guide a collective approach to seize this opportunity for impact.

There is, therefore, a responsibility on philanthropy to support this work over the next two years and beyond.

Annexes

I. **Implementation processes**: this table authored by ECNL by provides a detailed outline of key implementation processes, their significance to fundamental rights and opportunities for civil society engagement.

II. **Implementation timeline**: this timeline provides an overview of key implementation processes and when they are planned to take place.

III. **Case studies: national-level enforcement of the AI Act in the Netherlands and Spain**: the two case studies examine the national enforcement landscape in Spain and the Netherlands, looking at the regulatory authorities that might be engaged in AI Act enforcement, and doorways for civil society participation.

European
Artificial Intelligence
& Society Fund