Commentary

European Partnership for Democracy

Democracy and Electoral Processes: A Missed Opportunity for the EU General-Purpose AI Code of Practice?

2 September 2025

The EU **Code of Practice on General-Purpose AI** is a voluntary framework developed by the European Commission in collaboration with industry, civil society, and other stakeholders to promote the responsible development and deployment of general-purpose AI systems. The Code aims to establish common principles and risk mitigation measures for GPAI models, particularly in areas where their use may pose systemic societal risks, including to democratic processes. It is designed to complement the implementation of the Artificial Intelligence Act (AI Act), the EU's new legal framework for AI, which entered into force in August 2024.

At the European Partnership for Democracy, we have previously raised concerns that the AI Act does not provide **adequate protection for electoral integrity**, even though the protection of democracy is cited as one of its main objectives. In practice, it is very difficult to categorise AI applications related to elections as either prohibited or high-risk under the Act, due to narrow definitions that effectively exclude most AI systems used in electoral contexts from its scope.

Some AI applications relevant to elections-such as systems for voter data analysis and predictive analytics used for microtargeting-could arguably be **considered as prohibited** under the scope of Article 5.1(a) on subliminal techniques and Article 5.1(b) on exploiting vulnerabilities to distort behaviour. However, the requirements under these provisions are very strict, particularly with regard to demonstrating 'significant harm' and proving a direct causal link between the system and the harm. The recently published Guidelines on Prohibited AI Practices offer little clarification or additional guidance on these issues.

Furthermore, in Annex III 8(b), the AI Act identifies **certain AI systems linked to elections[1] as high-risk,** but only if they are 'intended' to influence elections and are not merely organisational tools. This limitation could exclude systems that clearly pose a threat, such as those used for political microtargeting or generating deepfakes, since it is difficult to prove the intent of a system that might have multiple uses, including non-political ones.

Rules for **General-Purpose AI (GPAI) applications** also do not explicitly address the use of AI to influence elections. In this context, the Code of Practice, even as a voluntary instrument, represented an opportunity to strengthen protections specifically regarding the risks GPAI poses to democratic processes. The Code was finalised and published on 10 July 2025.

While we welcome the explicit reference to "democratic processes" and "harmful manipulation" in the final version of the Code as an essential starting point, the current framing **remains too vague to capture the depth and complexity of risks that GPAI poses to democracy**, particularly regarding electoral integrity and civic participation. The following sections outline several areas where more detailed and precise framing is urgently needed.

1. Insufficient specification of democracy-related risks

The General-Purpose AI Code of Practice lists the promotion of democracy, rule of law, and fundamental rights among its key objectives. However, democracy-related risks are only mentioned in Appendix 1.4 of the Annex, under the category of 'harmful manipulation'[2]. Appendix 1.1 on Types of Risks refers more broadly to '(4) Risks to fundamental rights' and '(5) Risks to society as a whole'.

While including 'democratic processes' under the harmful manipulation category is a step in the right direction, the language used remains abstract and lacks actionable clarity. To ensure meaningful risk mitigation, the taxonomy should identify concrete threats that GPAI systems pose to democratic processes, particularly elections. These include:

- **Vote suppression and influence**: AI-generated personalised political ads, deepfake messages, and synthetic voice calls may be used to discourage voter turnout or manipulate voter preferences, especially among vulnerable or marginalised groups.
- **Disinformation campaigns**: GPAI can fabricate election-related content-such as fake

[1] "AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda. This does not include AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise and structure political campaigns from an administrative and logistic point of view."

[2] (4) Harmful manipulation: Risks from enabling the strategic distortion of human behaviour or beliefs by targeting large populations or high-stakes decision-makers through persuasion, deception, or personalised targeting. This includes significantly enhancing capabilities for persuasion, deception, and personalised targeting, particularly through multi-turn interactions and where individuals are unaware of or cannot reasonably detect such influence. Such capabilities could undermine democratic processes and fundamental rights, including exploitation based on protected characteristics.

news about candidates, campaign platforms, or voting procedures-posing a direct threat to informed voter choice and public trust.

- **Forgery of election data**: Generative AI could be exploited to produce fake election records that mimic official documents or datasets, undermining the credibility of election outcomes.

- **Erosion of civic discourse**: GPAI may replicate and amplify societal biases, marginalising certain voices and reducing pluralistic engagement. Smear campaigns targeting civil society actors further threaten inclusive participation.

- **Opaque use by public administration**: When governments deploy GPAI tools without transparency regarding data sources or decision-making logic, it creates accountability gaps and undermines democratic oversight.

To improve the taxonomy, the Code of Practice should follow the structure of the Digital Services Act (DSA) by explicitly including "civic discourse and electoral processes" as a systemic risk category. The *Liberties-EPD-DSA Risk Analysis* offers a strong foundation for doing so, including examples of relevant systemic risks. Additionally, sub-categories under existing risk headings could more explicitly reflect democracy-related harms. We recommend the following changes:

- **New category on civic discourse and electoral processes**: Add a distinct category encompassing electoral integrity, civic participation, and public trust; and in particular the risks outlined above.

- **Subcategories under existing risks**:

    - *Cyber offence*: Include explicit references to threats against public administration systems and electoral infrastructure (e.g. voter database hacking).
    - *Harmful manipulation*: Include AI-enabled disinformation, political ads microtargeting, and multi-modal influence operations (e.g. deepfakes, synthetic voice). Also incorporate AI applications for policy development, election observation, and civic engagement.

2. Strengthening mitigation measures

The GPAI CoP currently under-specifies mitigation measures tailored to democratic contexts. To address this, the following actions should be explicitly included:

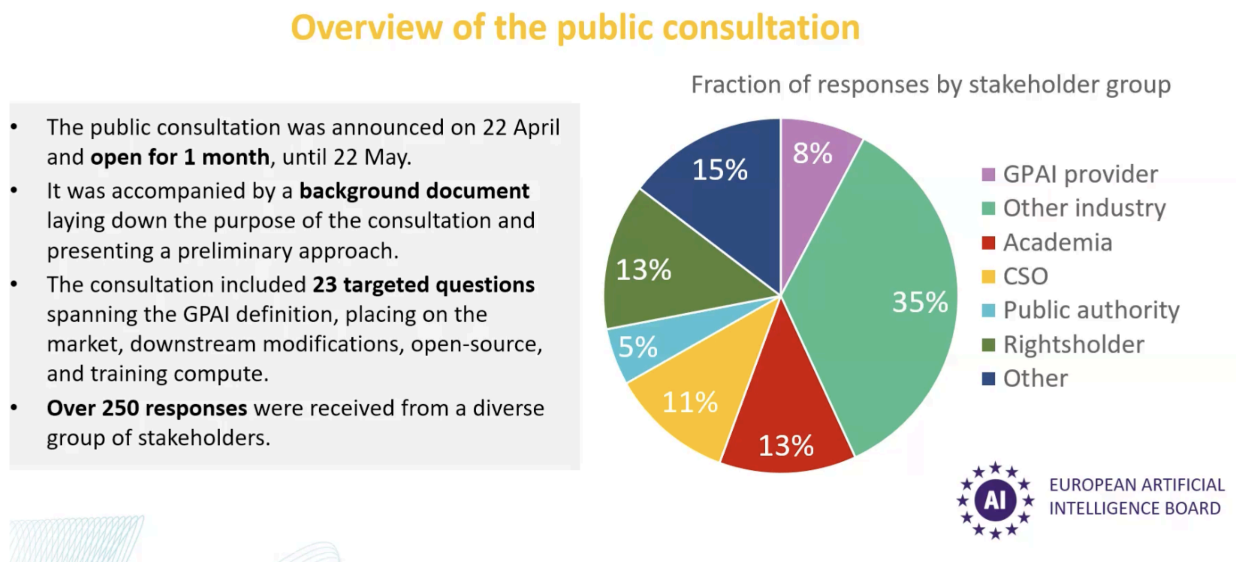
- **Watermarking and provenance tools:** To identify AI-generated political content, especially during election campaigns.
- **Feature limitations on political content:** Restrict certain generative features-like deepfake creation and hyper-personalisation-in electoral contexts.

- **Promotion of accurate information:** Encourage GPAI systems to prioritise verified, non-partisan data sources in civic applications.
- **Bias auditing and inclusive dataset design:** Ensure GPAI tools used in public-facing contexts do not reinforce harmful biases.
- **Public sector protocols:** Develop clear internal policies for GPAI use in public administration, including algorithmic impact assessments and transparency safeguards.
- **Robust detection mechanisms:** Require deployment of advanced detection tools, particularly for use by election authorities and watchdogs.
- **Transparency obligations:** Developers should provide documentation on data sources, model limitations, and intended use cases for GPAI in public sector settings.

3. Process concerns and civil society marginalisation

While the EU's stated goal for the drafting of the Code of Practice was to include various stakeholders, the actual process fell short-particularly with regard to civil society participation. In particular, we identified:

- **Limited civil society input:** Only 11% of participants represented civil society organisations, while nearly half were from industry. The ambiguous "other" category raises further concerns about transparency and balance.



Overview of the public consultation

- The public consultation was announced on 22 April and **open for 1 month**, until 22 May.
- It was accompanied by a **background document** laying down the purpose of the consultation and presenting a preliminary approach.
- The consultation included **23 targeted questions** spanning the GPAI definition, placing on the market, downstream modifications, open-source, and training compute.
- **Over 250 responses** were received from a diverse group of stakeholders.

Fraction of responses by stakeholder group

- **Unrealistic deadlines:** Compressed feedback windows and ineffective meetings made meaningful participation nearly impossible for under-resourced civil society actors.
- **Lack of transparency in revisions:** It remains unclear how CSO feedback was incorporated, with little evidence of substantive integration.

- **Tokenism risks:** If structured this way, participatory efforts risk becoming performative rather than genuinely consultative.

4. Voluntary commitments and effective enforcement mechanisms

The decision by companies like Meta to decline signing the Code of Practice already highlights the fundamental limitations of relying on non-binding instruments in areas of high societal impact.

While voluntary codes of conduct can play a constructive role-particularly in early stages of regulatory development-their effectiveness is inherently constrained by the absence of enforceability. This is especially problematic in mature, high-stakes domains such as elections, civic discourse, and political advertising, where risks are well documented. Continued reliance on soft law in these areas delays meaningful accountability and undermines public trust.

The fact that major actors can opt out of the Code without consequence further reinforces the need for binding legal frameworks to ensure consistent compliance and protect the public interest. In a democratic system like the EU, soft law should serve as a complement, not a substitute for enforceable regulation.

Conclusions & recommendations

The GPAI CoP is a welcome initiative, but it does not go far enough to protect democratic processes from the growing risks posed by General-Purpose AI. We urge the European Commission and other stakeholders to revise the Code with clearer risk categorisation, more robust mitigation strategies, and a stronger commitment to inclusive, participatory development. Electoral integrity, civic engagement, and democratic accountability cannot be afterthoughts; they must form the foundation of Europe's AI governance.

Given the growing body of evidence on AI-related harms in electoral contexts, the CoP must be significantly strengthened as part of the review outlined in Article 56(8)[3] of the AI Act. Without such improvements, both the Code and the AI Act risk becoming a missed opportunity to defend Europe's democratic resilience in the AI era.

[3] 1. The AI Office shall, as appropriate, also encourage and facilitate the review and adaptation of the codes of practice, in particular in light of emerging standards. 2. The AI Office shall assist in the assessment of available standards.