

Intentionality Unlocked: the European Commission's Guidelines on High-Risk AI Systems

3 September 2026

The European Commission has [released](#) draft **Guidelines on the classification of high-risk AI systems** as part of the implementation of the [Artificial Intelligence Act](#) (AI Act), the new EU Regulation introducing rules for AI systems according to their risk level.

In the AI Act, the rules on high-risk AI systems - which are only allowed on the EU market after undergoing a risk assessment - are particularly relevant for **democratic processes** because of their impact on election integrity. In particular, high-risk AI systems include **AI systems intended to be used to influence elections** in Annex III 8b, namely as:

“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.”

In a previous analysis, we [assessed](#) that the AI Act does not seem protective enough when it comes to election integrity, as it is very difficult to include any sort of AI application in the high-risk category, because of the **requirement of “intentionality”**. Even some AI systems that would naturally be included (e.g. microtargeting of political ads) hardly fit in the very narrow definitions provided by

the AI Act. We had therefore recommended to include specific clarifications in the **Guidelines on high-risk and non-high-risk use cases** foreseen under Article 6.5.

Now, the European Commission has published [draft](#) Guidelines on the classification of high-risk AI systems. The Guidelines bring **welcome clarifications** on the different high-risk cases and related legal interpretation, with concrete examples of what would be included in scope - and what wouldn't - and a **much broader scope for inclusions than what was expected**. The final guidelines will be **adopted by the end of 2026** and the application of the rules on high-risk AI systems will run as of December 2027 for standalone AI systems and August 2028 for AI embedded in other products.

In the next section, we will analyse the Guidelines with a specific focus on Annex III 8b on AI systems intended to be used to influence elections.

Main elements and steps forward in the Guidelines

The Guidelines on the classification of high-risk AI systems represent a **highly comprehensive legal tool** that takes into account a wide range of practical cases.

The Guidelines highlight that for an AI system to be classified as high-risk in the context of elections, two conditions must be met: first the system must be directly intended at influencing elections; and second persons should be directly exposed to the outputs of the system. In particular, the guidelines offer welcome **clarity on "intentionality"**, which is clarified both as a concept and via case-by-case analysis.

“the AI system would have to be specifically intended to have an effect on the electorate’s choice or turnout, fall within the scope of the use case listed in point 8(b) of Annex III. The focus of the use case is thus on underlying objectives: the system must be directed towards electoral influence, not merely be incidentally capable of it.”

The **examples given as excluded** are “general content recommender systems that, amongst other content, also recommend political content” even though, the text states, they “de facto, have the potential to influence political opinions”; and “general-purpose AI systems, which offer sufficient safeguards against a use influencing electoral processes” (see more on use cases below).

The text also clarifies further what “**influencing the outcome of an election**” and “**voting behaviour**” mean using a broad interpretation that doesn't rely on these elements to be demonstrable or effective, but just based on intentionality.

The Guidelines also address **deployer-neutrality**, i.e. that classification doesn't depend on *who* deploys the system (political party, third-party agency, advocacy group etc.), closing a possible reading where only campaigns themselves would be caught.

Additionally, it is important to see a dedicated section on the **interplay between AI Act prohibitions and other key EU legislation**, such as the [Digital Services Act](#) (DSA), the [Political Ads Regulation](#) (TTPA) and the Democracy Shield. This alignment is essential for regulatory coherence, as AI technologies often operate at the intersection of multiple legal frameworks.

Finally, **use cases** are clarified in extensive detail, both those included and excluded as part of Annex III 8b. We will look into the different use cases in the next section.

Use cases included and not included

Based on the criteria outlined above (intentionality and direct exposure of natural persons to the output), the draft Guidelines **exclude the following systems**:

- **systems that are not directly ‘intended’ to be used to influence elections**, for instance:
 - “**general recommender systems** that, amongst other content, also recommend political content and thus, de facto, have the potential to influence political opinions”
 - “**general-purpose AI systems, which offer sufficient safeguards** against a use influencing electoral processes:
 - **a chatbot clearly replying that it cannot give any voting advice** when asked by a user,
 - **[a chatbot] providing only neutral, factual, and informational content** about elections (voting procedures (how, when, where), registration procedures; the institutional and legal framework; objective information on parties and candidates (e.g. references to their official websites); and general civic education on democratic processes.”

- **systems that persons are not directly exposed to, such as tools used at organisational level**, for instance:
 - optimising campaign staff/logistics
 - analysing donor data
 - generating campaign material
 - monitoring elected officials
 - presenting information for academic use
 - and counting ballots.

Systems falling within point 8(b) and hence included are as follows:

- **AI-enabled targeting of political ads**, intended to optimize the targeting and ad delivery of political advertising, including specialised recommender systems
- **AI-enabled chatbot intended to promote support for candidates or policies**: a chatbot (or a virtual spokesperson/agent) developed for use by political actors to interact with natural persons in a conversational manner, simulating political dialogue with voters to persuade them to support a candidate or policy
- **Voter advice applications**: an AI system designed to recommend political parties or candidates based on an individual voter's views, for example asking natural persons interacting with the system a set of questions about political preferences, values, or political issues and then comparing the answers with the positions of political parties or candidates, presenting the 'closest match'

Based on our previous analysis as well as on the clarifications provided by the Guidelines, however, we recommend that the **following applications should be included, excluded or clarified**:

Include	1) AI systems for voter data analysis and predictive analytics ("Cambridge Analytica-style" systems). The Guidelines' example of sociological agencies (on excluded uses) suggests such analysis is out of scope where it "informs" only. We think this needs nuance: the same analytical system is often a direct input into microtargeting or campaign strategy, and in those cases it should be treated as in scope, since it is a functional step towards influencing voting behaviour, not a neutral research output. We recommend clarifying that whether such systems are in or out of scope depends on whether their output feeds directly into voter-facing influence activities, not merely on the analytical technique used.
---------	---

Exclude	1) AI systems used to identify cyberattacks against election IT infrastructure (e.g. voter registration databases, e-voting systems). Out of scope: their purpose is protecting system integrity, not influencing outcomes or voting behaviour, and voters are not directly exposed to their output. 2) AI systems used to maintain or verify voter eligibility lists. Similarly out of scope: their function is administrative/verificatory, not to shape electoral choice or turnout, even though errors could indirectly affect participation.
Clarify	1) General purpose chatbots: According to the text, the high-risk category seems to extend to general-purpose chatbots under specific conditions: if such a chatbot lacks a safeguard preventing it from answering election-related questions, it can be treated the same as a dedicated voter advice tool, and therefore fall within scope. This clarification is welcome but somewhat buried in the drafting rather than stated as a clear rule. It remains unclear how far it extends to general-purpose chatbots more broadly, and a more explicit statement would improve the reach of the text to catch a variety of types of chatbots that can influence voter behaviour. 2) Content-moderation/recommender systems that are specifically tuned to prioritise, suppress or amplify electoral content (distinct from the "general recommender" example given). "Specialised recommender systems" are mentioned as part of the included category of AI-enabled political ads - for more clarity we do however recommend that these would be in scope as a separate category, clarifying that a recommender system is not always "general purpose" but can have a concrete impact on voter behaviour.

Conclusions & recommendations

Overall, the draft Guidelines are a positive step forward. It is welcome to see **concrete use cases actually spelled out**, rather than the provision being left to abstract wording: the clarifications on intentionality, the worked examples, and the interplay with adjacent regulation all represent a meaningful improvement in legal certainty.

Other than looking closely at the additional use cases suggested above, the point on **chatbots also deserves further attention**. This is not a marginal issue: there is growing evidence of the extent to which chatbots are being used in electoral contexts, and of their real capacity to influence voter behaviour and opinion formation.

Given this, the Guidelines should state more explicitly how and when general-purpose chatbots fall within the scope of point 8(b), including what safeguards would be sufficient to keep a system out of scope.