



# POLICY BRIEF

15 05 2024

13

## CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK AND RELEVANT OBLIGATIONS UNDER THE AI ACT

ARIANNA ROSSI



Classification of AI systems as high-risk and relevant obligations under the AI Act	
BACKGROUND AND FIELD OF APPLICATION	<p>The AI Act is a <b>risk-based regulation</b>, that identifies various categories of risks that AI systems can engender and therefore assigns <b>corresponding regulatory burdens</b> to their providers.</p> <p>Following classical definitions in business management, cybersecurity and data protection, risk is defined as “<b>the combination of the probability of occurrence of harm and the severity of harm</b>” (Article 2(5)(g)(1)).</p> <p>The AI Act establishes prohibitions on systems that bear an unacceptable risk, <b>many obligations for developers and deployers of high-risk AI systems</b>, and some obligations for AI systems bearing residual risk.</p> <p>This policy brief only concerns high-risk AI systems.</p>
HIGHLIGHTS	<p>AI systems are categorized as high-risk (Article 6) whenever:</p> <ul style="list-style-type: none"> <li>(a) they are <b>used as safety components or a product</b> and need a <b>third-party conformity assessment</b>, thus fall under the EU’s product safety legislation (see Annex II), such as medical devices; or</li> <li>(b) they are used in the following <b>domains</b> (listed in Annex III):             <ol style="list-style-type: none"> <li>1) systems for remote biometric identification, biometric categorisation based on sensitive attributes and emotion recognition;</li> <li>2) management and operation of critical digital infrastructure;</li> <li>3) education and vocational training (e.g., admission, learning outcomes evaluation);</li> <li>4) employment, worker management and access to self-employment (e.g., recruitment, termination of contract);</li> <li>5) access to and enjoyment of essential private services and essential public services and benefits (e.g., eligibility for public assistance services, creditworthiness);</li> <li>6) law enforcement (e.g., assessing likelihood of offence);</li> <li>7) migration, asylum and border control management (e.g., eligibility for asylum);</li> <li>8) administration of justice and democratic processes (e.g., legal interpretation, dispute resolution).</li> </ol> </li> </ul> <p>High-risk systems need to comply with <b>requirements</b> on risk management (Article 9), data governance (Article 10), technical documentation (Article 11), record-keeping (Article 12), transparency (Article 13), human oversight (Article 14), and accuracy, robustness and cybersecurity (Article 15).</p>
IMPACT ON PROJECT	<p>In the case of AI systems that are developed for medical purposes and need a CE mark (i.e., medical devices), these will certainly be categorized as high-risk AI systems and will need to respect the requirements listed above. This is relevant even for researchers, since the <b>decisions taken at</b></p>



**the development stage should be accurately documented** to foster transparency and informed use, and to provide the necessary technical documentation that is necessary to demonstrate compliance.

For example, the **transparency** requirements of article 13 impose that developers of high-risk AI systems disclose information on the intended purpose, technical capabilities, input data and performance of the system on certain groups or persons, among the others. Information that helps deployers understand the output and deploy the system correctly should also be disclosed to avoid misuse (we refer to Policy Brief no 12 for further information about transparency).

Moreover, **documentation** should be provided to demonstrate compliance with the AI Act's provisions (Article 11) and should contain, among others, details about the expected outcomes, the system architectures, the employed datasets, the monitoring, functioning and control of the AI system, such as its capabilities and limitations in performance and the foreseeable unintended outcomes and sources of risks. Requirements on **human oversight** and **data governance** (see also Policy Brief 14 on Data governance) also require gathering information about the functioning of the system early on.