




AI ACT ACCURACY, ROBUSTNESS AND CYBERSECURITY

- Title I: General Provisions
- Title II: Prohibited AI Practices
- Title III: **High-risk systems**
- Title IV: Transparency obligations for certain systems
- Title V: Measures in support of innovation 
- Title VI: Governance
- Title VII: EU database for stand-alone high-risk AI systems
- Title VIII: Post-market monitoring, information sharing, market surveillance
- Title IX: Codes of Conduct
- Title X: Confidentiality and penalties

Chapter 2

Requirements for high risk systems



Chapter 2

Art. 15

Accuracy, robustness and cybersecurity

1. High-risk AI systems shall be **designed and developed** in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and **perform consistently** in those respects throughout their lifecycle.
2. The **levels of accuracy and the relevant accuracy metrics** of high-risk AI systems shall be declared in the accompanying instructions of use.

Chapter 2

Art. 15

Accuracy, robustness and cybersecurity

3. High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems.



The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans.

High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations ('feedback loops') are duly addressed with appropriate mitigation measures.

Chapter 2

Art. 15

Accuracy, robustness and cybersecurity

4. High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities.

The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.

The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws.

A golden statue of Lady Justice, blindfolded and holding scales of justice in her left hand and a sword in her right hand, set against a blue sky background.

- HumanE-AI-NET

- AI Act: enables, prohibits, restricts
 - *Reasonable?*
 - *Pertinent?*