

# EU AI Act cheat sheet

## An overview of the Act

The **EU AI Act** aims to make Europe a leader in AI, balancing benefits and risks. It focuses on protecting human rights and ensuring AI systems are safe, ethical, and trustworthy. The Act imposes strict requirements on high-risk AI systems, including risk management and cybersecurity, and seeks to reduce burdens on businesses to foster innovation. It also addresses issues like bias and potential misuse of AI, requiring thorough testing and monitoring.

Scope

✓ **Providers:** Applies to those placing AI systems or models on the EU market, regardless of location

✓ **Authorised representatives:** Covers representatives of non-EU established providers

✓ **Deployers:** Includes users of AI systems either within the EU or outside, if the output is used in the EU

✓ **Importers and distributors:** Encompasses those involved in bringing AI systems into the EU market

✓ **Product manufacturers:** Applies to those placing an AI system together with their product on the EU market, and under their own name or trademark

Timeline

August 1, 2024:

 EU AI Act implementation begins

February 2, 2025:

 Compliance with Chapters I and II on prohibited AI uses; includes national law integration for real-time biometric AI use authorisation and incident reporting

August 1, 2026:

 Introduction of rules for Annex III high-risk AI systems and establishment of regulatory sandboxes

August 2, 2025:

 Enforcement of regulations for general-purpose AI models; mandates notification to EU Commission and adherence to Chapter V requirements

August 2, 2027:

 Activation of rules for Annex I high-risk AI systems plus those for high-risk AI systems that are not prescribed in Annex III but are intended to be used as a safety component of a product

4 risk categories

1. Unacceptable risk:

 AI systems that pose a clear threat to safety, livelihoods, and rights, such as social scoring and biometric categorisation, are prohibited

2. High risk:

 AI systems that serve as a safety component listed in Annex I, or the AI system is intended for high-risk use cases specified in Annex III in specific sectors including education, employment, law enforcement and migration

3. Limited risk:

 AI systems that interact with individuals or generate content, posing impersonation or deception risks, must meet specific transparency requirements

4. Minimal or no risk:

 Applications like AI-enabled video games or spam filters, considered risk-free, are freely used but must comply with data protection laws

### High-risk AI systems: Key requirements overview

Providers

- Establish a continuous risk management system
- Ensure robust data governance
- Maintain comprehensive technical documentation.
- Implement a quality management system
- Conduct conformity assessments
- Register the AI system in the EU AI database.
- Accountability framework confirming management responsibilities
- Provide sufficient transparency to enable deployers to interpret a system's output and use it appropriately
- Designed so that human oversight can be implemented
- Providers in third countries must appoint an authorised EU representative

Deployers

- Ensure transparency and explainability of the AI system.
- Perform fundamental rights impact assessments.
- Ensure compliance and monitoring in accordance with the provider's instructions
- Adequate AI literacy
- Human oversight by natural persons
- Incident reporting
- Cooperation with the authorities

### Compliance processes

Providers

- Complete a conformity assessment before placing a high-risk AI system on the market, which can be done internally or by a third-party body in specific cases
- Make a legal declaration of compliance and notify the relevant national authority
- Register the AI system in the EU AI database after declaring conformity
- Retain technical documentation and logs for 10 years after the AI system is placed on the market
- Implement a comprehensive Quality Management System, including regulatory compliance strategies, design and quality assurance procedures, data management, risk management, post-market monitoring, and incident reporting
- Establish a post-market monitoring system to ensure continuous compliance and take corrective actions if necessary

Deployers

- Ensure AI literacy among their staff and take into account the technical knowledge and context of the AI systems
- Perform fundamental rights impact assessments for high-risk AI systems used in public services, creditworthiness evaluations, and insurance risk assessments

Deployers should be aware that they will still have other obligations under EU or member state law in addition to those in the AI Act, such as those under the GDPR.

### Penalties and enforcement mechanisms

**For prohibited AI practices:** Fines can reach up to **€35 million or 7% of global annual turnover**, whichever is higher. This penalty is applicable for non-compliance with the prohibition of certain AI practices deemed too risky or harmful.

**For value-chain member failures:** Entities within the AI value chain that fail to meet their obligations may face fines up to **€15 million or 3% of global annual turnover**.

**For misleading information:** Providing incorrect or misleading information to notified bodies or national competent authorities can result in fines of up to **€7.5 million or 1% of global annual turnover**.

### Key steps towards AI governance

01

Identification of all AI systems

02

Risk classification of AI systems

03

Understanding AI Act requirements and obligations

04

Build an AI governance framework and implement controls

05

Ongoing monitoring of compliance

### Stay ahead of the curve with BoardEffect

BoardEffect, part of the Diligent One Platform, provides innovative boardroom technology for volunteer boards and mission-driven organisations. It helps you manage risk, keep up with regulations and delivers clear insights in one view, so leaders can make informed decisions quickly.

For more information or to request a demo: [sales@boardeffect.com](mailto:sales@boardeffect.com)