ICTRECHT

NL AI Coalitie

Cheat sheet

AI Act

Everything you need to know about the new rules for AI and algorithms.

Read more

Scope

01 Definition of AI

AI systems that, for implicit and explicit objectives, with a degree of autonomy, infer for themselves which output to generate.*

*The AI Act contains separate rules for general-purpose AI models.

02 Territorial

Providers placing AI systems on the EU market (regardless of their place of establishment), deployers, importers, distributors, and authorized representatives (of providers).

03 Who

Manufacturers, sellers, distributors, and deployers.

04 Exceptions

Exceptions include private use in a household context, military applications and national security, law enforcement (in part), scientific research, and open source (very limited).

Risk levels

01 Unacceptable risk (prohibited)

Manipulative or deceptive techniques, exploitation of vulnerabilities, social scoring, emotion recognition in the workplace, facial recognition databases, and real-time remote biometric identification (for law enforcement).

02 High risk

Based on the Union harmonisation legislation listed in Annex I to the AI Act:

(Safety components of) regulated products such as medical devices, machinery, motorized vehicles, lifts, toys, etc.

Based on use cases listed in Annex III to the AI Act:

Biometrics, critical infrastructure, education and vocational training, employment, essential services and benefits, law enforcement, administration of justice, and migration, asylum and border control. Unless the AI-system:

- Only improves human activity.
- Only performs a limited procedural task.
- Does not influence decisions.
- Carries out only preparatory tasks.

03 Transparency risk (low risk)

AI systems that interact directly with individuals (including chatbots), generative AI (text, images, audio, etc.), emotion recognition and biometrics (where permitted).

04 Residual category (minimal or no risk)

AI systems that do not fall within the other risk categories.

Compliance: high-risk AI-systems

Documentation

Clear and specific technical documentation and instructions for use.

Riskmanagement and quality management system

Identify, assess, manage, and mitigate potential risks. Safeguard quality.

Fundamental Rights Impact Assessment (FRIA)

Carry out a structured analysis of risks to fundamental rights.

Post-market monitoring

Establish a system to collect and analyse data on the performance of the AI system throughout its lifecycle.

Transparency

Ensure explainability, automatic logging and record-keeping.

Conformity assessment

Affix the CE mark once full compliance with the AI Act has been achieved.

Human oversight

Ensure human involvement in the process (in-the-loop) or close supervision (in command).

Accuracy, robustness and cybersecurity

Reduce the risk of biased outputs, ensure resilience against errors and failures, and protect against cyber threats and misuse.

Data governance

Manage the representativeness, quality and lawfulness of data.

AI with transparency risks:

- Inform individuals that they are interacting directly with AI.
- Label the output of generative AI.
- Inform individuals about the use of biometrics and emotion recognition (where permitted).

General-purpose AI models

- Make technical documentation and summaries of training data available.
- Adopt a policy to ensure compliance with copyright law. Comply with codes of practice.
- Large AI models with ‘systemic risk’ must carry out additional evaluations and implement additional safeguards.

Fines and enforcement

Each Member State must designate at least one supervisory authority. In the Netherlands, the existing market surveillance authorities and inspectorates will supervise AI.

Supervisory authorities may:

- Require access to all documentation, source code and model parameters.
- Issue binding instructions regarding adjusted use.
- Order cessation if the AI system proves too risky.
- Impose fines.

When does the AI Act apply?

12 June 2024

Publication in the Official Journal.

1 August 2024

Entry into force of the AI Act. The rules apply in phases.

2 February 2025

- Prohibition of unacceptable AI.
- AI literacy obligations apply.

2 May 2025

Deadline for publication of codes of practice for general-purpose AI models.

2 August 2025

Rules apply regarding:

- General-purpose AI models.
- Conformity assessment bodies.
- Fines.
- Deadline for publication of fining guidelines.
- Deadline for establishing supervisory authorities (and implementing procedures).

2 August 2026

- Fully applicable to all forms of AI (except Annex I) and certain legacy IT systems.
- Deadline for publication of guidelines on post-market monitoring.

2 August 2027

Rules for high-risk AI systems under Annex I apply.

1 January 2030

The AI Act applies to certain large-scale government IT systems (Annex X to the AI Act).

Fines may amount to:

EUR 35 million

or, for undertakings, 7% of worldwide annual group turnover for the use of prohibited AI.

EUR 15 million

or, for undertakings, 3% of worldwide annual group turnover for other infringements.

EUR 7.5 million

or, for undertakings, 1.5% of worldwide annual group turnover for providing incorrect, incomplete or misleading information to supervisory authorities.

Lower maximum amounts will apply to SMEs and start-ups.

ICTRECHT

NL AI Coalitie

Would you like to know more about the AI Act?

Visit our website for the latest news, our services and training courses.

Questions?

- https://www.ictrecht.nl/en/ai-act
- 020 663 1941