

# AI Act of the European Union

## Rules for trustworthy AI

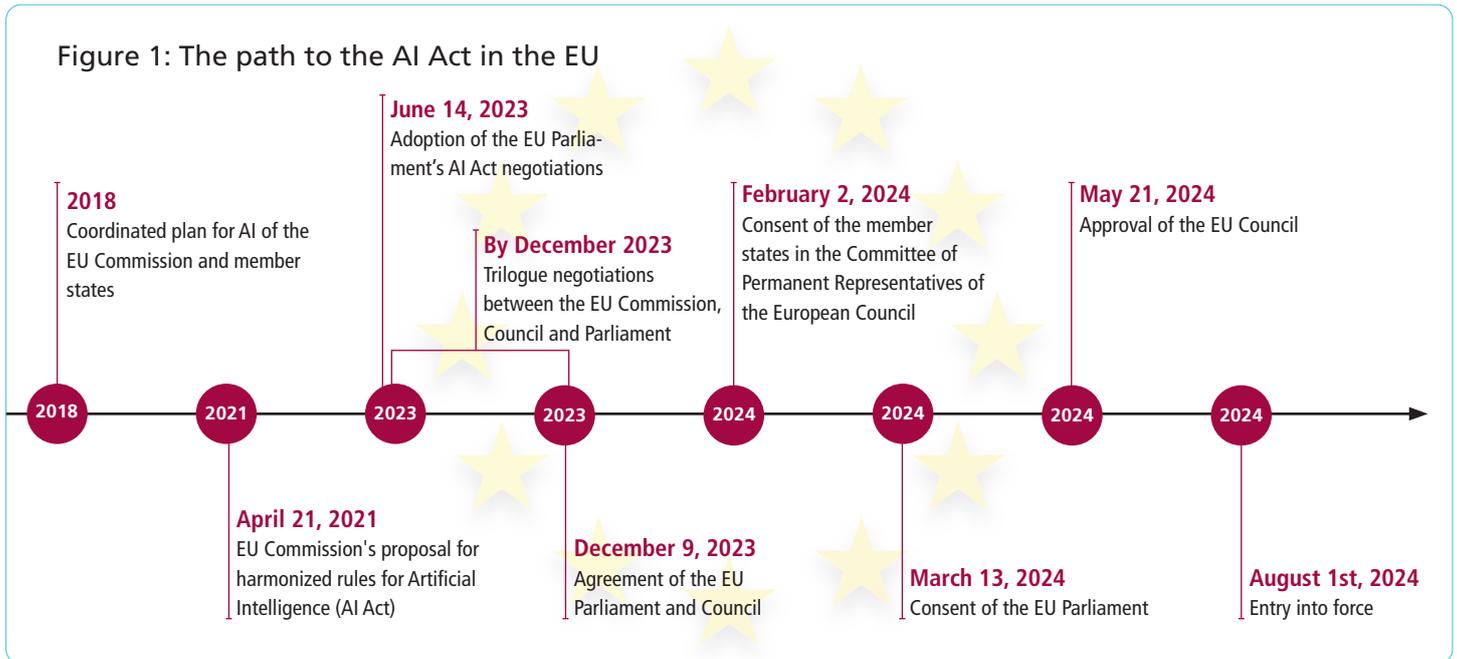
### AT A GLANCE

- The AI Act creates a **uniform, binding legal framework** for the **trustworthy use of AI** in the EU.
- The regulation **bans** AI systems with unacceptable risks. This includes real-time **bio-metric surveillance** in public spaces.
- **High risk AI systems** must meet certain safety requirements before they can be placed on the EU market.
- **General purpose AI (GPAI) models** such as ChatGPT are regulated in a tiered approach depending on their computing power.
- **Potential:** protection of fundamental rights, legal certainty, “AI made in Europe” as a competitive advantage
- **Challenges:** inhibiting innovation due to legal hurdles, incomplete ban on biometric real-time monitoring, different application of the regulation in member states

## What is the AI Act?

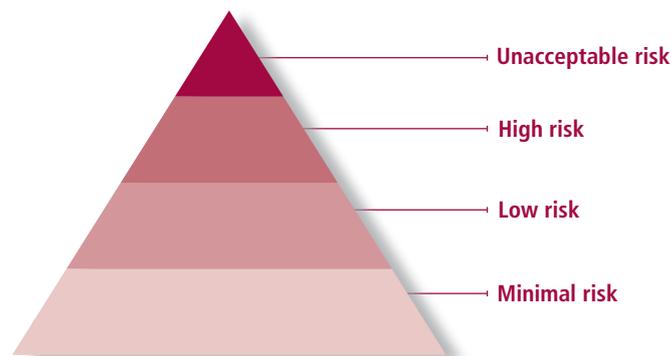
The **Artificial Intelligence Act**, or **AI Act for short**, is the European Union (EU) regulation for Artificial Intelligence (AI). It sets out clear rules for the development and use of AI systems and thus creates a **uniform, binding legal framework** in the EU. The aim is to create trustworthy AI that is used in accordance with European values. AI systems used in the EU should be safe, transparent, ethical, impartial and under human control. At the same time, the AI regulation is intended to keep AI **technology** and **research competitive within the EU** and promote innovation. The regulation is the first transnational AI regulation of its kind in the world.

Figure 1: The path to the AI Act in the EU

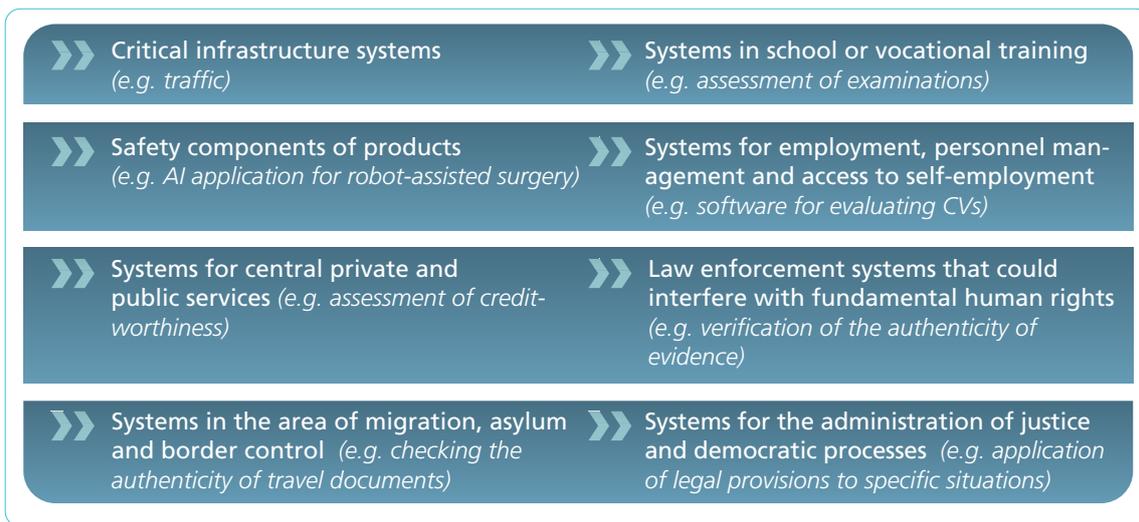


## How does the AI Act regulate the use of AI?

The EU regulates Artificial Intelligence according to its risk potential. The AI Act distinguishes between four risk groups for which different regulations apply.



- **Unacceptable risk:** All AI systems that fall into this category are generally prohibited. This includes all applications that pose a clear threat to EU citizens, such as manipulative and exploitative AI systems. The list of prohibited practices contained in the AI Act includes, for example, assessments of social behaviour with data that is evaluated beyond the context in which it was collected (so-called social scoring), or the bio-metric identification of people in real time (exceptions exist for counter-terrorism).
- **High risk:** AI systems in this category require careful testing before they can be put into operation, as well as further checks during their service life. High risk AI systems include products – and their safety components – that are regulated in certain other EU regulations and directives, such as the Medical Devices Regulation. In addition, all stand-alone AI systems that fall into the following categories are, in principle, high risk applications:



Providers of high risk AI systems must carry out a multistage review of their system before they are allowed to launch it on the market.

- **Low risk:** AI systems that fall into this category are subject to low transparency obligations. The aim is to give users an overview of how the system works. The decision on whether to continue using the application is therefore up to the citizens. One example of this is automated movie or music recommendations.
- **Minimal risk:** This includes systems that pose only a minimal or no risk to fundamental rights. They are not subject to any regulations. This category includes most AI systems, such as AI-supported video games. Providers of such systems can voluntarily submit to codes of conduct. This means that products with minimal risk can also meet some or all of the requirements of the AI Act.

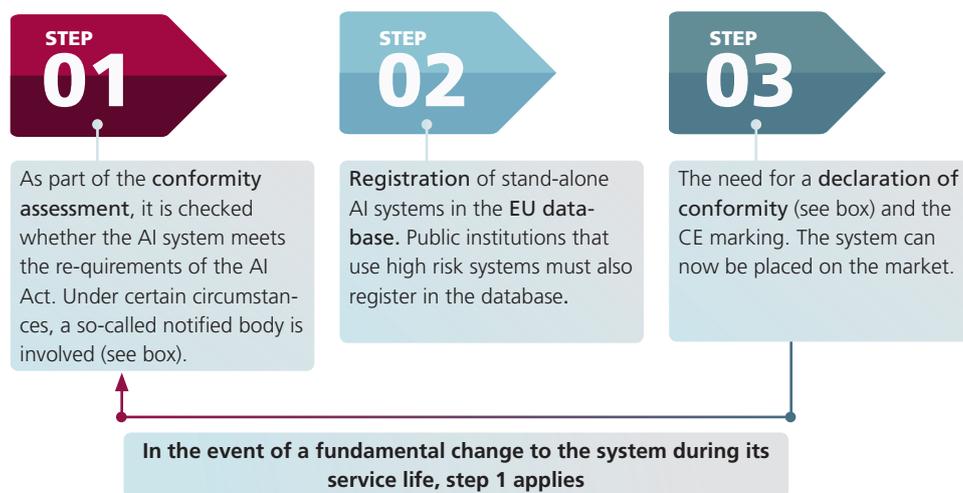
### Testing of high risk AI systems

The AI Act imposes strict requirements on AI systems that pose high risks. These include, among other things:

- Establishment of a **risk management system**, i.e. a regular and systematic review and update throughout the life cycle of a high risk system that identifies known and foreseeable risks to health, safety or fundamental rights (Art. 9).
- Fulfillment of **quality criteria for the training data sets** of the AI systems, which, among other things, must be representative and largely error-free and avoid bias that can lead to discrimination (Art. 10).
- Provision of **technical documentation** prior to placing on the market that provides the necessary information in a clear and comprehensive manner to assess the compliance of the system with the requirements of the AI Act (Art. 11).
- Technically enabling the **automatic recording of events** (“logs”), e.g. malfunctions during the entire service life of the system (Art. 12).
- Provision of **instructions** for use with appropriate transparency, explaining the mode of operation with concise, complete, correct and clear information (Art. 13).

- Enabling effective **human supervision** of AI systems during their use. This includes a “stop button” with which the system can be brought to a standstill in a safe state at any time (Art. 14).
- Consideration of **benchmarks and measurement methods** to achieve an appropriate level of accuracy, robustness and cybersecurity, for example through appropriate measures against feedback loops with biased results (Art. 15).
- Establishment of a **quality management system** that ensures compliance with this regulation (Art. 17).

Before a provider can bring a high risk AI system onto the market in the EU, it must check whether its system complies with the requirements of the AI Act.



### Conformity assessment

AI systems with high risks must undergo a conformity assessment. There are basically two procedures for assessing conformity:

- internal control by the manufacturer itself or
- evaluation of the quality management system and the technical documentation with the involvement of a state-authorized inspection body, the so-called notified body.

Notified bodies must be involved in all biometric applications (i.e. systems for the automated remote identification of persons or for emotion recognition) and if, for example, there are no harmonized standards that the manufacturer can use to justify compliance. In all other cases, manufacturers assess the conformity of their AI system internally. The EU Commission is thus taking into account the problem that there is currently still a lack of expertise and standards in the relevant institutions that would be suitable for an external assessment. In the case of AI systems that have to undergo a conformity assessment as product components or products in accordance with another EU product directive, the notified bodies designated for these regulations and directives are also responsible for the conformity assessment of the AI component.

## Key points of the AI Act

In addition to the general provisions, the definition of prohibited AI systems and the classification into risk levels, the AI Act contains specific regulations for implementing the ordinance.

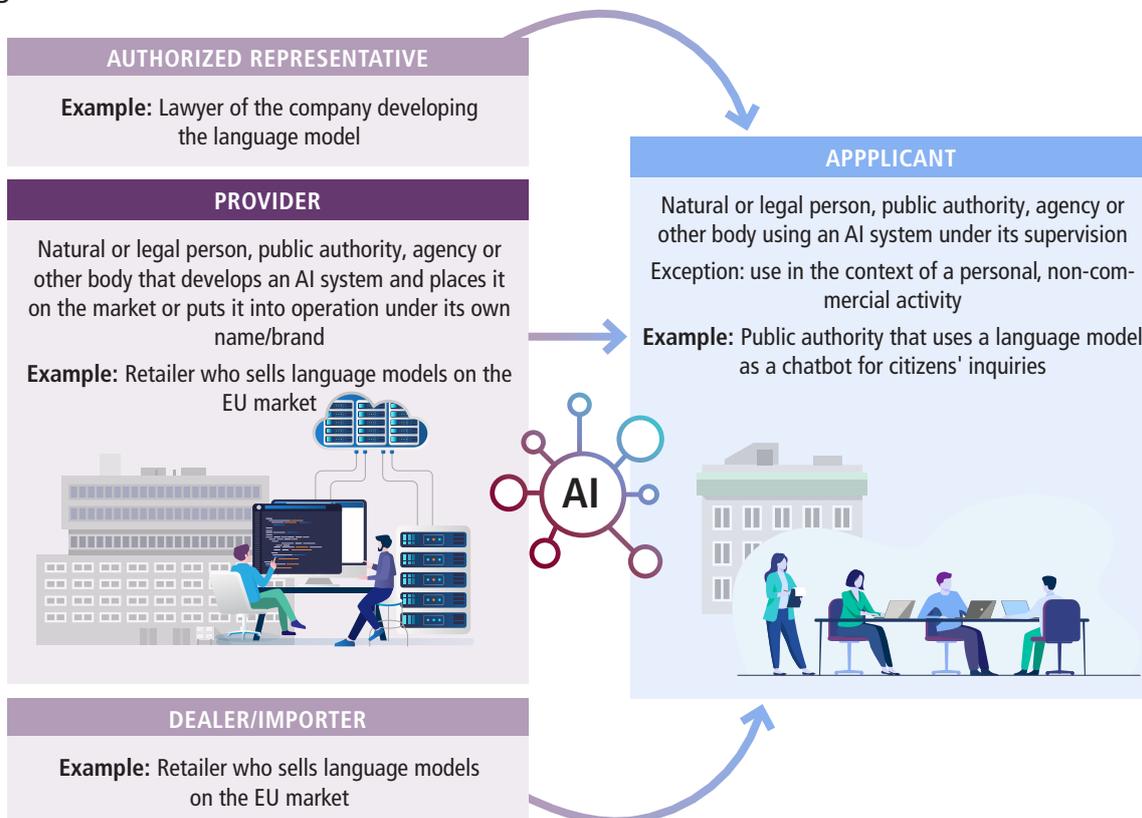
### Definition of AI

An AI system is a machine-based system that is designed to operate with varying degrees of autonomy, that can demonstrate adaptability after its initial deployment, and that derives from the input it receives for explicit or implicit goals how to produce outcomes **such as predictions, content, recommendations or decisions that can influence** the physical or virtual environment.

### Areas of application

The regulation only applies to areas of application of EU law (i.e. not to areas of responsibility of the member states or areas of national security). It does not apply to AI systems that serve military or defense policy purposes. AI systems that are developed and put into operation for the sole purpose of research and development or that are used for research, testing or development activities before being placed on the market or put into operation are also excluded from the regulation. Persons who use AI systems for non-commercial purposes are also exempt from the regulation.

Figure 2: Addressees of the AI Act



### Promotion of innovation

Companies, especially small and medium-sized enterprises (SMEs) and start-ups, should be able to develop, test and validate innovative AI systems in so-called regulatory sand-boxes under real-life conditions. These real-world laboratories – i.e. experimental environments – must meet certain safeguards. In addition, the fees for the conformity assessment of innovative AI systems for SMEs are to be kept low and special advice centers for SMEs are to be set up in the member states.

### AI systems with general purpose and open source models

The AI Act is intended to take account of the variety of possible uses of AI systems. For example, no specific use is initially envisaged for basic AI models, which form the basis for all generative AI applications. However, they could later be integrated into a high risk system. Special regulations therefore apply to such general purpose AI (GPAI) models: Providers must ensure transparency by creating technical documentation on the training and test procedures used as well as the training data and prove that they comply with European copyright law. The regulation differentiates between GPAI models depending on their computing capacity: very powerful models with a computing capacity of more than  $10^{25}$  FLOP are subject to stricter rules, as they can pose systemic risks that spread depending on their subsequent application. The additional obligations relate to cyber security and energy efficiency, for example.

The obligations set out in the regulation also apply to all open source models that fall into the group of prohibited or high risk systems, as well as to GPAI models that are published under open source licenses, insofar as they pose a systemic risk. Open source models that pose no or low risks are exempt from the AI regulation.

### Governance architecture

An AI Office is to be set up at the EU Commission. This is to monitor the most advanced AI models, promote standards and test procedures and enforce the regulations in the member states (see p. 8). A scientific panel of independent experts will advise the office on general purpose AI models. An AI committee with representatives from the member states will act as a coordination platform and advisory body for the Commission. Technical expertise will be made available to the committee through an advisory forum of various stakeholders.

In addition, each member state will set up at least one authorized inspection body and a market surveillance authority to implement the regulation at national level. The national authorities can provide guidelines and advice on the implementation of the AI Act, especially for SMEs and start-ups.

### Transparency obligations

As a general rule, it should always be clear to all people when they come into contact with AI. Providers of AI systems that are intended for direct interaction with natural persons must ensure at the development stage that those affected are informed that they are communicating with an AI system. Anyone using an AI system that generates or manipulates image, audio or video content (deep fake) must also disclose that the content was created artificially and label it as such in a machine-readable format.

Codes of conduct and test procedures are being developed at EU level to facilitate the labeling of artificially generated or manipulated content.

## Sanctions

Fines for violations of the AI Act can be imposed up to an upper limit of either 7 percent of the company's global annual turnover or EUR 35 million, whichever is higher. The lower of these fines applies to SMEs and start-ups. In future, natural or legal persons will be able to submit complaints about AI systems to the market surveillance authority.

### Case study: Biometric facial recognition

Biometric facial recognition in real time is prohibited if it is used to monitor or discriminate against people. For law enforcement authorities, the use of biometric facial recognition is permitted under certain conditions if strict security regulations are adhered to: If there is a specific threat, the authorities may biometrically identify individuals in public spaces. This requires prior official or judicial approval and is only intended for a strictly defined list of criminal offenses. Such systems may be used, for example, to specifically search for a missing person or a person who has committed an offense specified in the ordinance or to prevent a terrorist attack. There are also temporal and spatial restrictions. High risk systems that have not passed the conformity assessment procedure may also be used for law enforcement in these urgent cases.

The subsequent evaluation of biometric data collected in public spaces is classified as a high risk application, but is generally permitted. Court approval is required for this. Law enforcement authorities can track down criminals in this way, subject to strict safeguards.

## The AI Act as part of the European digital strategy

The AI Act is part of the EU's digital strategy. Its aim is to make new technologies safe and easy to use for private individuals and companies and to contribute to climate neutrality. In addition to the AI Act, the EU's digital strategy includes other regulations that are relevant to the regulation and design of AI systems.



In addition, individual areas of technology are already regulated by specific regulations in the EU and at national level, such as the European Medical Device Regulation (MDR). In the case of an AI-based medical device, the AI Act will also apply in future. Last but not least, certain high risk systems such as autonomous driving are also regulated by standards such as ISO/PAS 8800.

## Potential and challenges

The AI Act is an important step towards comprehensive regulation of Artificial Intelligence in the EU. However, there are also concerns and challenges associated with the Act.

Potentials	Challenges
<p><b>Trustworthy AI:</b> The fundamental rights of every human being are comprehensively protected by the AI Act. The AI Act creates transparency for users. It prescribes legal standards in line with European values for high risk AI systems.</p>	<p><b>Biometric surveillance through the back door:</b> Critics complain that the exceptional cases in which biometric real-time surveillance by law enforcement is permitted are too extensive.</p>
<p><b>Uniform legal framework:</b> As an EU regulation, the AI Act applies in all EU member states. It provides companies with binding rules for the development and use of AI systems.</p>	<p><b>Unequal application:</b> There are concerns that the review of compliance with the law could lead to different approaches between the various member states.</p>
<p><b>Innovation and competitiveness:</b> The AI Act creates protected spaces in which companies can test their innovations. Internationally, the quality feature of trustworthy "AI made in Europe" could also prove to be a competitive advantage.</p>	<p><b>Barriers to innovation:</b> Critics fear that the AI Act could hamper AI innovations, especially in small and medium-sized enterprises. The reason for this is the potentially high cost of complying with the provisions of the AI Act.</p>
<p><b>Technological sovereignty:</b> The AI Act differentiates between GPAI models depending on their computing capacity: stricter rules apply to very powerful models. This opens up fair opportunities for European providers of smaller models in international competition.</p>	<p><b>Inadequate risk classification for GPAI models:</b> Critics complain that the calculation figure alone is not a suitable yardstick for deriving the potential risks of a model.</p>

## What happens next?



Once adopted, the AI Act will set the framework for the regulation of AI in Europe. Standards regulate exactly how the regulation is to be implemented in various fields of application. The EU Commission has commissioned the European standardization institutions CEN and CENELEC to develop the basic requirements for AI systems set out in the AI Act in more technical detail, e.g. for autonomous driving. The Commission will review the finalized standard. If the result is positive, the standard will become a so-called harmonized European standard. Anyone who complies with it may assume that they meet the requirements of the AI Act covered by the respective standard in this field of AI application. The application of standards remains voluntary.

The CEN members – including the German Institute for Standardization DIN – must adopt the European AI standards unchanged in their national standards and withdraw conflicting national standards. This means that the same European standards apply in all EU member states. However, the member states are free to go beyond the standard and issue stricter national regulations.

## Evaluation: Voices from Plattform Lernende Systeme



*The AI regulation is a pioneer: it represents the world's first attempt to guarantee the safety of AI systems ex ante. However, the definition of which information systems fall under the central concept of an AI system is complex: these should be systems with different degrees of autonomy that do not operate solely on the basis of rules created by humans. However, according to the recitals, knowledge- or rule-based expert systems should certainly be covered by the regulation, and the specification and application to specific borderline cases is left to case law.*

**Prof. Dr. Ruth Janal**, University of Bayreuth

*AI is a tool by and for people that can simplify and make our lives easier. When using AI, we should therefore prioritize the opportunities over the potential risks and exploit them within the framework of the law and our European value system. In order to achieve this goal, it is necessary to define, implement and monitor AI from the planning stage ("ethics by design") through all phases of the life cycle.*

**Bernhard Hünsgberg**, Deutsche Telekom AG



*The AI Act obliges providers of generative AI solutions to be transparent. In the context of high scalability, the obligation to label synthetic data is not only sensible, but also essential to curb misinformation. Responsible providers such as Brighter AI already label the works created with the help of their AI application as such. However, the AI Act raises public awareness of these and other challenges. Against the backdrop of this debate about the risks of AI and their categorization in the AI Act, best practices and standards for dealing with the technology will emerge in the best case.*

**Marian Gläser**, Brighter AI Technologies GmbH

## Further reading

**European Commission:** Artificial Intelligence – Excellence and Trust.

Online at: [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence\\_de#f%C3%BCr-mehr-exzellenz-im-bereich-ki](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_de#f%C3%BCr-mehr-exzellenz-im-bereich-ki)

**European Commission (21.04.2021):** Proposal for a Regulation of the European Parliament and the Council.

Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts.

Online at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

**European Commission Europe's Digital Decade:** digital goals for 2030.

Online at: [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en)

**European Commission, Directorate-General for Communication Networks, Content and Technologies (2019):**

Ethical guidelines for trustworthy AI. Online at: <https://data.europa.eu/doi/10.2759/22710>

**European Council (09.12.2023):** Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in

the world. Online at: [Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world – Consilium \(europa.eu\)](https://www.consilium.europa.eu/en/press/press-releases/2023/12/09-artificial-intelligence-act-council-parliament-strike-a-deal-on-the-first-rules-for-ai-in-the-world/)

**European Parliament (19.04.2024):** Artificial Intelligence Act. Corrigendum. Online at:

[https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf)




---

Content from AI AT A GLANCE may be used for editorial purposes provided the source Plattform Lernende Systeme is acknowledged.

---

### Imprint

Expertise: Bernhard Hüngsberg, Ruth Janal, Frauke Rostalski

Editors: Alexander Mihatsch, Linda Treugut, Erduana Wald

Editorial staff: Lernende Systeme – Germany's Platform for Artificial Intelligence | Managing Office | c/o acatech | Karolinenplatz 4 | D-80333 Munich  
kontakt@plattform-lernende-systeme.de | www.plattform-lernende-systeme.de

Status: May 2024 | Photo credits: iStock/Hasan As Ari/p. 5; Freepik/p. 5; Vuk Latinovic, Privat, Brighter Technologies GmbH/p. 9

Follow us on [X](#) and [LinkedIn](#).

SPONSORED BY THE



Federal Ministry  
of Education  
and Research

**acatech**  
NATIONAL ACADEMY OF  
SCIENCE AND ENGINEERING

## Further sources and further reading

**Think digital** Artificial Intelligence Act. Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz). Online at: <https://eu-digitalstrategie.de/ai-act/>

**Future of life Institution** EU Artificial Intelligence Act. Entwicklungen.

Online at: <https://artificialintelligenceact.eu/developments/>

**Lilian Edwards (2022)** The EU AI Act: a summary of its significance and scope

**Tagesspiegel Background (24.11.2023)** KI – Regulierung. Berlin, Paris und Rom wollen Selbstregulierung für GPT & Co.

Online at: <https://background.tagesspiegel.de/digitalisierung/berlin-paris-und-rom-wollen-selbstregulierung-fuer-gpt-co>

**Europäische Kommission** Ein Europa für das digitale Zeitalter.

Online at: [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age\\_de](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_de)

**OECD** Empfehlung des Rats zu künstlicher Intelligenz.

Online at: [https://www.oecd.org/berlin/presse/Empfehlung-des-Rats-zu-kuenstlicher-Intelligenz.pdf?\\_ga=2.11476669.809215705.1702550541-1051922027.1702550541](https://www.oecd.org/berlin/presse/Empfehlung-des-Rats-zu-kuenstlicher-Intelligenz.pdf?_ga=2.11476669.809215705.1702550541-1051922027.1702550541)

**Think digital** Gesetze der EU – Digitalstrategie. Gesetze im Überblick.

Online at: <https://eu-digitalstrategie.de/data-act/>

**Europäische Kommission** Europäisches Daten-Governance-Gesetz.

Online at: <https://digital-strategy.ec.europa.eu/de/policies/data-governance-act>

**Europäische Kommission** Das Digital Service Act Paket.

Online at: <https://digital-strategy.ec.europa.eu/de/policies/digital-services-act-package>

**Europäische Kommission** Das EU-Cybersicherheitsgesetz.

Online at: <https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-act>

**Amtsblatt der Europäischen Union (5.4.2017)** Verordnungen. Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates. Online at: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017R0745>

**German AI Association (July 2023)** The EU AI Act. Towards the finish line: Key Issues and proposals for the trilogue negotiations

**European Commission (9.12.2023)** Commission welcomes political agreement on Artificial Intelligence Act.

Online at: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_6473](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473)