The EU Artificial Intelligence Act

Updated, 2 February 2024

The EU institutions are now moving forward with an updated and "final" text of the Artificial Intelligence (AI) Act, following December's political agreement and further technical meetings in January.

The AI Act is a landmark in global AI regulation, reflecting the EU's objective to lead the way in promoting a comprehensive legislative approach to support the trustworthy and responsible use of AI systems. The AI Act follows other major EU digital legislation, such as the General Data Protection Regulation (GDPR), the Digital Services Act, the Digital Markets Act, the Data Act, and the Cyber Resilience Act.

This paper outlines key elements of the AI Act as it currently stands and provides an overview of the Act's tiered compliance obligations.

This paper does not constitute legal advice.

The AI Act will unify how AI is regulated across the single market of the 27 EU Member States. It also has important extraterritorial implications, as it covers *all AI systems impacting people in the EU*, regardless of where systems are developed or deployed.

Compliance obligations are significant, and largely determined by the level of risk the usage of an AI system poses to people's safety, security, or fundamental rights. Obligations apply along the AI value chain. The AI Act applies a tiered compliance framework. Most requirements fall upon the developers and deployers of AI systems classified as "high-risk", and on general-purpose AI systems (including foundation models and generative AI systems) posing "systemic risks".

The agreement currently sets out a phased timeline for enforcement, starting with prohibited AI systems in late 2024 / early 2025 and progressively extending to nearly all AI systems by mid-2027. There are significant financial penalties for noncompliance.

It is important for business leaders in the EU and beyond to consider the implications of this complex legislation before it comes into effect. This consideration includes understanding how the AI Act interacts with existing and emerging rules and regulations in other jurisdictions, as well as with voluntary AI codes and principles.

Businesses and other organizations should ensure they have an up-to-date inventory of the AI systems that they are developing or deploying. They will need to assess whether their systems are subject to compliance obligations and, if so, under which classification. Developers and deployers of high-risk and general-purpose AI systems will also need to ensure that effective AI governance frameworks and compliance systems are in place.

Key takeaways

Who will the AI Act affect?

- The AI Act applies to all AI systems impacting people in the EU (whether these AI systems are built and operated from within the EU or from elsewhere). It applies across all sectors.
- The AI Act imposes different obligations across all actors in the AI value chain.
- In certain cases, the AI Act also applies to AI models and systems placed on the market prior to the Act taking effect, including:
    - If these are General Purpose AI (GPAI, see definition below) models.

- If these are AI systems which fall into the "prohibited" category, or if these are "high-risk" AI systems that are intended to be used by public authorities.
- Moreover, if an existing AI system undergoes significant changes, it will be treated like the other systems in its "updated" risk category that are being placed on the market at the same time.

What are the key features of the AI Act?

- **Definition of AI**: The AI Act applies a broad definition of an AI system derived from the recently updated Organization for Economic Co-operation and Development definition (see relevant section below).
- **Risk-based approach focuses on use cases**: Obligations are primarily based on the level of risk posed by how an AI system is used (or could be used), not the technology on which it is based.
  - GPAI models are treated separately due to the breadth of their potential use cases.
- **Risk classification system**: The AI Act establishes a tiered compliance framework consisting of different categories of risk and different requirements for each such category. All AI systems will need to be inventoried and assessed to determine their risk category and the ensuing responsibilities.
  - **Prohibited systems**: Systems posing what legislators consider an unacceptable risk to people's safety, security and fundamental rights will be banned from use in the EU.
  - **High-risk AI systems**: These systems will carry the majority of compliance obligations (alongside GPAI systems - see below), including the establishment of risk and quality management systems, data governance, human oversight, cybersecurity measures, post-market monitoring, and maintenance of the required technical documentation. (Further obligations may be specified in subsequent AI regulations for healthcare, financial services, automotive, aviation, and other sectors.)
  - **Minimal-risk AI systems**: Beyond the initial risk assessment and some transparency requirements for certain AI systems, the AI Act imposes no additional obligations on these systems but invites companies to commit to codes of conduct on a voluntary basis.
- **Pre-market conformity assessments for high-risk AI systems**: High-risk systems will require a conformity assessment to evidence their compliance before being placed on the market:
  - The application of harmonized standards (currently under development, see below) will allow AI system providers to demonstrate compliance by self-assessment.
  - In limited cases, a third-party conformity assessment performed by an accredited independent assessor ("notified body") will be required.
- **General purpose AI systems (GPAI), including foundation models and generative AI**: These advanced models and systems will be regulated through a separate tiered approach, with additional obligations for models posing a "systemic risk".
- **Measures to support innovation**: Regulatory "sandboxes" will be made available across the EU for operators (especially small and medium enterprises) to access voluntarily. Here they can innovate, experiment, test, and validate the compliance of their AI systems with the AI Act in a safe environment.
- **Interaction with other EU laws**: Obligations under the AI Act will need to be integrated into the compliance processes already established to implement existing EU laws, e.g., laws regarding product safety, privacy, and financial services.
- **Enforcement and penalties**: National competent authorities will have enforcement powers with the capacity to impose significant fines depending on the level of noncompliance.
  - For use of prohibited AI systems, fines may be up to 7% of worldwide annual turnover (revenue), while noncompliance with requirements for high-risk AI systems will be subject to fines of up to 3% of the same.

When will the AI Act take effect?

- The Act is currently expected to enter into force in Q2-Q3 2024, with different obligations then taking effect in stages. Some key dates are outlined below:

- AI Act prohibitions will start to be enforced six months after the Act enters into force (Q4 2024 – Q1 2025).
- GPAI obligations will take effect 12 months after entry into force (Q2-Q3 2025), but with one exception: GPAI models which have been placed on the market before this date will have an additional 24 months to comply (so from Q2-Q3 2027).
- Most other obligations will take effect 24 months after the Act enters into force (so, Q2-Q3 2026).
- However:
    - Obligations for AI systems that are classified as high-risk because they are a safety component of a system that is subject to Union harmonization legislation (listed in Annex II), will only take effect 36 months after the Act enters in force (so from Q2-Q3 2027).
    - Obligations for high-risk AI systems intended for use by public authorities that were on the market before the entry into force of the AI Act, will only take effect 48 months after entry into force (so from Q2-Q3 2028).

What actions should companies and other organizations take from the outset?

1) Inventory all AI systems you have (or potentially will have) developed or deployed and determine whether any of these systems falls within the scope of the AI Act.
2) Assess and categorize the in-scope AI systems to determine their risk classification and identify the applicable compliance requirements.
3) Understand your organization's position in relevant AI value chains, the associated compliance obligations and how these obligations will be met. Compliance will need to be embedded in all functions responsible for the AI systems along the value chain throughout their lifecycle.
4) Consider what other questions, risks (e.g., interaction with other EU or non-EU regulations, including on data privacy), and opportunities (e.g., access to AI Act sandboxes for innovators, small and medium enterprises, and others) the AI Act poses to your organization's operations and strategy.
5) Develop and execute a plan to ensure that the appropriate accountability and governance frameworks, risk management and control systems, quality management, monitoring, and documentation are in place when the Act comes into force.

Context

The AI Act is intended to advance four key objectives:[1]

(i) To ensure that AI systems placed on the EU market are safe and respect fundamental rights

(ii) To ensure legal certainty to facilitate investment and innovation in AI

(iii) To enhance governance and effective enforcement of EU law on fundamental rights and safety requirements applicable to AI systems

(iv) To facilitate the development of a single market for lawful, safe and trustworthy AI applications, and prevent market fragmentation

Who is affected?

The AI Act is broad in scope and comes with significant obligations along the value chain. It focuses on the impact of AI systems on people, specifically on their wellbeing and fundamental rights.

It also contains extraterritorial measures, affecting any business or organization that offers an AI system impacting people within the EU, regardless of where the organization is headquartered.

Under certain conditions the AI Act also applies to AI systems that were put on the market prior to the Act taking effect:

- If these are GPAI models.
- If these are AI systems which fall into the "prohibited" category, or if these are "high-risk" AI systems that are intended to be used by public authorities.
- Moreover, if an existing AI system undergoes significant changes, it will be treated like the other systems in its "updated" risk category that are being placed on the market at the same time.

The AI Act will apply to (please see the appendix section below for full definitions of terms):

- Providers putting AI systems on the market within the EU, regardless of their location
- Providers and deployers of AI systems located in a non-EU country, where the output of the AI system is used within the EU
- Deployers of AI systems located in the EU
- Importers and distributors placing AI systems on the EU market
- Product manufacturers placing products with AI systems on the EU market under their own name or trademark

The AI Act will **not** apply to:

- Public authorities in non-EU countries and international organizations that have law enforcement and judicial cooperation agreements with the EU, provided that adequate safeguards are in place
- AI systems used for purposes outside the scope of EU law-making authority, such as military or defense
- AI systems specifically developed and used for the sole purpose of scientific research and discovery
- Research, testing and development activity regarding AI systems prior to placement on the market or into service
    - Free and open-source software, unless their use would classify them as a prohibited or high-risk AI system, or their use would subject them to transparency obligations

[1] "EU AI Act Proposal, 2021 – Explanatory Memorandum", European Commission, April 2021 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206

When will the AI Act be implemented?

The AI Act is expected to be approved by the European Parliament and Council and published in the Official Journal in Q2-Q3 of 2024, after which it will come into force. As an EU regulation (as opposed to a directive), it will be directly effective in Member States without the need for local enabling legislation.

The timeline for compliance with the provisions of the AI Act will be as follows:

Timeframe	Development
Calendar Q2-Q3 2024	AI Act expected to come into force.
Immediately after entry into force	The European Commission must begin work to establish the AI Office (EU oversight body) while Member States make provisions to establish AI regulatory sandboxes. (To note: the work to establish the AI Office has already begun).
Six months after entry into force (Q4 2024 – Q1 2025)	AI Act prohibitions will come into effect.
12 months after entry into force (Q2-Q3 2025)	Requirements for GPAI models will come into effect. However, GPAI models that were already on the market before this date will have an additional 24 months to comply (see below).
24 months after entry into force (Q2-Q3 2026)	Requirements for high-risk AI systems (classified under uses listed in Annex III) will come into effect, alongside transparency requirements for certain other AI systems.
36 months after entry into force (Q2-Q3 2027)	Requirements for high-risk AI systems classified under EU harmonization laws contained in Annex II will come into effect. GPAI models that were already on the market before obligations began to apply twelve months after entry into force (see above), will now have to comply.
48 months after entry into force (Q2-Q3 2028)	High-risk AI systems intended for use by public authorities that were on the market before the entry into force of the AI Act should now be compliant.

How does the EU define an AI system?

The AI Act's definition of an AI system is derived from the recently updated definition used by the Organisation for Economic Co-operation and Development (OECD). The objective in using the OECD definition as a basis, is to encourage international alignment and continuity with other laws and codes. The AI Act defines an AI system as follows:

> *"An AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."*

The AI Act emphasizes that a key characteristic that differentiates AI systems from simpler and more traditional software systems is their capability to infer. It states that the techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve a certain objective, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved. The capacity of an AI system to infer goes beyond basic data processing, enable learning, reasoning, or modelling.

How are AI systems classified?

The AI Act sets compliance obligations based on the inherent risks that arise from the application for which AI systems are used.

General-purpose AI systems (GPAI), including foundation models and generative AI systems, follow a separate classification framework. Please see the relevant section below.

AI systems are classified as follows in the Act:

Classification (Risk-based tier)	Description	Compliance level	Use case examples (see sections below for fuller details)
Prohibited AI systems	**Prohibited** because uses pose an unacceptable risk to the safety, security, and fundamental rights of people.	Prohibition	Includes use of AI for **social scoring** which could lead to detrimental treatment, **emotional recognition** systems in the workplace, **biometric categorization** to infer sensitive data, and **predictive policing** of individuals, among other uses. Some exemptions will apply.
High-risk AI systems	**Permitted,** subject to compliance with the requirements of the AI Act (including conformity assessments before being placed on the market).	Significant	Includes use of AI in: • **Recruitment**, • **Biometric identification surveillance** systems, • **Safety components of systems covered by harmonized legislation** (e.g., **medical devices, automotive**) • Access to essential private and public services (e.g., **creditworthiness, benefits, health and life insurance**), • **Safety of critical infrastructure** (e.g., **energy, transport**).
Minimal risk AI systems	**Permitted,** subject to specific transparency and disclosure obligations where uses pose a limited risk.	Limited	Certain AI systems that interact directly with people (e.g., **chatbots**), and visual or audio **"deepfake"** content that has been manipulated by an AI system.
	Permitted, with no additional AI Act requirements where uses pose minimal risk.	Minimal	By default, all other AI systems that do not fall into the above categories (e.g., photo-editing software, product-recommender systems, spam filtering software, scheduling software)

Prohibited systems: which use cases pose an unacceptable risk?

The AI Act prohibits AI systems that pose unacceptable risks and that can be used to undermine a person's fundamental rights, or that may subject them to physical or psychological harm. These prohibitions include:

- AI systems that exploit vulnerabilities, or deploy subliminal techniques, to manipulate a person or a specific group (e.g., children, the elderly, or people with disabilities), circumventing the users' free will in a manner likely to cause harm.
- AI systems used for the social scoring, evaluation, or classification of people based on their social behavior, inferred, or predicted, or personal characteristics, leading to detrimental treatment.

- AI systems used to infer emotions of people in the workplace (such as human resource functions) and educational institutions. Exemptions apply for some safety systems (e.g., detection of the drowsiness of pilots).
- Biometric categorization to infer sensitive data, such as race, sexual orientation, or religious beliefs.
- Indiscriminate and untargeted scraping of facial images from the internet or CCTV to populate facial recognition databases.
- Predictive policing of individuals, defined as predicting individual behavior such as individual likelihood of offense or re-offense.
- Law enforcement use of real-time remote biometric identification (RBI) systems in publicly accessible spaces (certain exceptions apply subject to prior judicial authorization and for strictly defined lists of criminal offenses).

High-risk systems: which use cases are subject to conformity assessments and obligations?

The AI Act identifies high-risk uses in Annex II and Annex III. The European Commission is empowered to update these annexes as new uses and risks are identified. The following high-risk uses are currently listed:

- AI systems used as a safety component of a product covered by EU harmonization legislation, including but not limited to:[2]
    - Medical devices
    - Motor vehicles
    - Machinery
    - Civil aviation
    - Marine equipment
    - Agricultural vehicles
    - Railway interoperability
    - Toys
- AI systems applied in uses that pose a significant risk of harm to health, safety, or fundamental rights:[3]
    - Biometric identification and categorization of people
    - Management and operation of critical infrastructure (specifically, safety components of traffic, water, gas, heating, and electricity infrastructure)
    - Education and vocational training (specifically, systems determining access to education and assessment of students)
    - Employment, worker management and access to self-employment (including recruitment and performance monitoring)
    - Access to and enjoyment of essential private and public services and benefits (including eligibility for benefits, evaluating creditworthiness, and pricing of life and health insurance, although those used for purposes of detecting financial fraud are specifically not included)
    - Law enforcement uses such as data analytics systems to assess evidence of criminal activity
    - Migration, asylum, and border control management (including monitoring of migration trends, border surveillance, verification of travel documents, and examination of applications for visas, asylum, and residence permits)
    - Administration of justice and democratic processes (including researching and interpreting the law)

Exceptions to high-risk classification:

However, an AI system will not be considered high-risk if it:

[2] Annex II, List of Union harmonisation legislation, EU Artificial Intelligence Act Proposal, Version 21 January 2024
[3] Annex III, High-risk AI systems referred to in Article 6(2), EU Artificial Intelligence Act Proposal, Version 21 January 2024

- Performs a narrow procedural task with no direct safety or security implications
- Is meant to review or improve the quality of human output
- Is used to detect decision-making patterns (or deviations from existing patterns to flag inconsistencies) without influencing decisions
- Is used for purposes of detecting financial fraud

What are the obligations for providers of high-risk AI systems?

General obligations

Requirements for high-risk AI systems include:

- Establishing and maintaining appropriate AI **risk** and **quality management systems**
- Effective **data governance**
- Maintaining appropriate **technical documentation** and **record-keeping**
- **Transparency** and provision of information to users
- Enabling and conducting **human oversight**
- Compliance with standards for **accuracy, robustness, and cybersecurity** for the intended purpose
- **Registering high-risk AI systems on the EU database** before placing them on the market; systems used for law enforcement, migration, asylum and border control, and critical infrastructure will be registered in a non-public section of the database

Pre-market conformity assessment for high-risk systems

Providers must perform a conformity assessment on the high-risk AI system before placing it on the market:

- The conformity assessment should examine whether the requirements laid out above have been met

In most cases, **providers can self-assess** if:

- They apply procedures and methodologies that follow EU approved technical standards (harmonized standards) that allow a presumption of conformity

A third-party conformity assessment by an accredited body (notified body) is required if any of the following criteria apply:

- The AI system is part of a safety component subject to third-party assessment under Union harmonized regulations (see above)
- The AI system is part of a biometric identification system
- Harmonized standards are not used

Post-market obligations

Once a high-risk AI system has been placed on the market, providers continue to have obligations to ensure ongoing safe performance and conformity over the system's lifecycle. These include:

- **Maintaining logs** generated by high-risk systems, to the extent that they are under their control, for a period of at least six months
- **Immediately taking the necessary corrective actions** for nonconforming systems already on the market and informing other operators in the value chain of the nonconforming systems
- **Cooperating with the national competent authorities or the AI Office** (see relevant section below) by sharing all the information and documentation necessary to show conformity upon receiving a reasonable request

- **Monitoring performance and safety** of AI systems throughout their lifetime and actively evaluating continuous compliance with the AI Act
- **Reporting to the appropriate authorities, serious incidents** and malfunctions that lead to breaches of fundamental rights
- **Undergoing new conformity assessments for substantial modifications** (e.g., changes to a system's intended purpose or changes that affect how it meets regulations):
  - This applies whether the changes are made by the original provider or any third party.
  - For AI systems that are considered to have limited or minimal risk, it will be important to check whether the original risk classification still applies after any changes.

What are the obligations for deployers, importers and distributors of high-risk AI systems?

Obligations of deployers of high-risk AI systems include:

- Completing a fundamental rights impact assessment (FRIA) before putting the AI system in use, if the deployer:
  - Is a public body or private entity providing public services
  - Provides essential private service that cover creditworthiness evaluation of persons, and risk assessment and pricing in relation to life and health insurance
- Implementing human oversight by people with the appropriate training and competence
- Ensuring that input data is relevant to the use of the system
- Suspending the use of the system if it poses a risk at a national level
- Informing the AI system provider of any serious incidents
- Retaining the automatically-generated system logs
- Complying with the relevant registration requirements when the user is a public authority
- Complying with GDPR obligations to perform a data protection impact assessment
- Verifying the AI system is compliant with the AI Act and that all relevant documentation is evidenced
- Informing people, they might be subject to the use of high-risk AI

Before placing a high-risk AI system on the market, it is the responsibility of importers and distributors to:

- Verify that the system complies with the AI Act, ensure that all relevant documentation is evidenced, and communicate with the provider and market surveillance authorities accordingly

Minimal-risk systems: what obligations apply?

For some specific AI systems, limited transparency obligations apply.

Providers must:

- Design and develop systems in a way to make certain that people understand that they are interacting with an AI system from the outset (e.g., chatbots)

Deployers must:

- Inform and obtain the consent of people exposed to permitted emotion recognition or biometric categorization systems (e.g., safety systems monitoring driver attentiveness)
- Disclose and clearly label where visual or audio "deep fake" content has been manipulated by AI.

How will general-purpose AI be regulated?

The definition in the AI Act of general-purpose AI (GPAI) models is:

> *"General-purpose AI model means an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This does not cover AI models that are used before release on the market for research, development and prototyping activities."*

The AI Act adopts a tiered approach to compliance obligations, **differentiating between high-impact GPAI models with systemic risk, and other GPAI models.** The AI Act defines "systemic risk at Union level" as:

> *"A risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the internal market due to its reach, and with actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain."*

The GPAI tiers are as follows:

Tier	Description	Compliance level
Base-level tier	Models meeting the GPAI definition	Limited transparency obligations
Systemic risk tier	High-impact GPAI models posing a systemic risk are provisionally identified based on cumulative amount of computing power used for training (with power greater than 10^{25} floating point operations [FLOPs]). A model can also be classified in this tier based on a decision of the Commission that a general-purpose AI model has capabilities or impact equivalent to those above.	Significant obligations

Providers of all GPAI models will be required to:

- Keep and maintain up-to-date technical documentation.
- Make information available to downstream providers who intend to integrate the GPAI model into their AI systems.
- Put in place a policy to respect EU copyright law.
- Disseminate detailed summaries about the content used for training.

Exceptions to base-level GPAI transparency obligations:

- Unless the GPAI models present systemic risks, these obligations shall not apply to providers of GPAI models that are made accessible to the public under a free and open-source license, and whose parameters are made publicly available.

In addition, providers of high-impact GPAI models posing a systemic risk must:

- Perform model evaluations.
- Assess and mitigate systemic risks.
- Document and report to the European Commission any serious incidents and the corrective action taken.
- Conduct adversarial training of the model (i.e., "red-teaming").
- Ensure that an adequate level of both cybersecurity and physical protections are in place.
- Document and report the estimated energy consumption of the model.

To provide agility for adapting to rapid GPAI technology developments, the AI Office (see relevant section below) will:

- Update the designation criteria for high-impact GPAI, with possible inclusion of criteria related to the number of model parameters, quality or size of datasets, number of registered business or end users.
- Facilitate the formulation of codes of practice to support the application of the compliance requirements.

How will the AI Act interact with existing legislation and standards?

- AI providers must continue to adhere to all relevant EU laws while incorporating requirements of the AI Act.
- Providers can combine AI Act compliance with existing procedures to avoid duplication and ease the compliance workload.
- Where applicable, the AI Act should be embedded into relevant EU laws (e.g., financial services regulations). Sectoral regulators will be designated as the relevant competent authorities to supervise the enforcement of the AI Act for their sector.

How will new standards be developed and when will they be ready?

To reduce compliance burdens and speed up time-to-market, the AI Act allows for compliance self-assessment, provided the obligations are met using European Commission-approved industry best practices as formalized in "harmonized standards".

- The European Commission has issued a "standardization request" to the European standards bodies (CEN and CENELEC), listing a series of topics for which new harmonized standards are required to cover the compliance obligations in the AI Act (see section on pre-market obligations of high-risk AI systems above).
- The European standardization bodies aim to have standards available in time for implementation of the AI Act in accordance with the agreed timelines (see above), but their readiness is not guaranteed.
- Where possible the European standardization bodies will seek to adopt standards created by the international standards bodies (ISO and IEC), with minimal modification.

Codes of Practice to support compliance with GPAI obligations

Providers of high-impact GPAI models posing a systemic risk may rely on codes of practice to demonstrate compliance until a harmonized standard is published.

The EU's new AI Office (see below) shall encourage and actively support the drawing up of codes of practice at Union level, to facilitate the effective implementation of the obligations regarding the detection and labelling of artificially generated or manipulated content. The Commission is empowered to adopt implementing acts to approve these codes of practice.

How does the AI Act aim to support AI innovation in the EU?

AI regulatory sandboxes

The AI Act mandates the establishment of AI regulatory sandboxes to offer innovation support across the EU.

- These regulatory sandboxes are **controlled environments** in which providers and deployers (e.g., small and medium enterprises) can voluntarily experiment, test, train, and validate their systems under regulatory supervision before placing them on the market.
- Each Member State will be expected to create a sandbox with common rules for consistent use across the EU.
- AI system providers will be able to receive a written report about their sandbox activities as evidence that they have met AI Act requirements. This is intended to speed up the approval process to take AI systems to market.

Real-world testing

Testing of AI systems in real-world conditions outside of AI regulatory sandboxes may be conducted by providers or prospective providers of the high-risk AI systems listed in Annex III of the AI Act (see above), at any time before being placed on the market, if the following conditions are met:

- A testing plan has been submitted to, and approved by the market surveillance authorities
- The provider is established in the EU
- Data protection rules are observed
- Testing does not last longer than necessary and no more than six months (with the option to extend by an additional six months)
- End users have been informed, given their consent and have been provided with relevant instructions
- The predictions, recommendations and decisions of the AI system can be effectively reversed or disregarded

What will the regulatory oversight model for the AI Act look like?

National competent authorities will be given oversight powers in Member States. These are likely to take different forms depending on the Member State.

At an EU level, the AI Act governance framework also establishes the:

- **AI Office** within the EU Commission, but with functional independence
  - This new body will have oversight responsibilities for GPAI models. It will contribute to the development of standards and testing practices, coordinate with the national competent authorities and help enforce the rules in Member States
- **AI Board** representing the Member States to provide strategic oversight for the AI Office
  - The Board will support the implementation of the AI Act and regulations promulgated pursuant to it, including the design of codes of practice for GPAI models
- **Scientific panel of independent experts** to support the activities of the AI Office
  - The panel will contribute to the development of methodologies for evaluating the capabilities of GPAI models and their subsequent classification, while also monitoring possible safety risks
- **Advisory forum** with representatives of industry and civil society
  - Will provide technical expertise to the AI Board

What are the penalties for noncompliance?

The AI Act sets out a strict enforcement regime for noncompliance.

There are three notional levels of noncompliance, each with significant financial penalties. Depending on the level of violation (in line with the risk-based approach), the Act applies the following penalties:

Noncompliance case	Proposed fine
Breach of AI Act prohibitions	Fines up to €35 million or 7% of total worldwide annual turnover (revenue), whichever is higher
Noncompliance with the obligations set out for providers of high-risk AI systems or GPAI models, authorized representatives, importers, distributors, users or notified bodies	Fines up to €15 million or 3% of total worldwide annual turnover (revenue), whichever is higher
Supply of incorrect or misleading information to the notified bodies or national competent authorities in reply to a request	Fines up to €7.5 million or 1.5% of total worldwide annual turnover (revenue), whichever is higher

In the case of small and medium enterprises, fines will be as described above, but whichever amount is lower.

National competent authorities will determine the fines in line with the guidance provided above.

What are the next steps around and beyond the AI Act?

The EU AI Act next steps:

Over the coming months the AI Act will be put to the European Parliament and Council for final approval.

It is currently expected that the Act will be approved by the end of April 2024, and then be published in the EU official journal in Q2-Q3 2024. The AI Act will come into force 20 days after publication, at which point the phased implementation timeline shall begin.

International alignment:

At an international level, the European Commission and other EU institutions will continue to work with multi-national organizations including the Council of Europe, the U.S.– EU Trade and Technology Council (TTC), the G7, the OECD, the G20, and the UN to promote the development and adoption of rules beyond the EU that are compatible with the requirements of the AI Act.

The EU AI Pact

The European Commission is planning to launch a voluntary AI Pact as soon as the AI Act is adopted. While a number of aspects of this proposed Pact are still to be clarified, it appears that it will seek the voluntary commitment of industry to start implementing some of the requirements of the AI Act ahead of the legal deadlines:

- The Commission will convene interested industry actors (EU and non-EU) in early 2024 to discuss the proposed AI Pact and start to exchange best practices.
- Once the AI Pact is launched, organizations will have the opportunity to sign-up and to make voluntary public commitments reflecting some of the steps they are taking to prepare for compliance with the AI Act.

Appendix

AI Act term	AI Act definition
Provider	A natural or legal person, public authority, agency, or other body that is or has **developed** an AI system to place on the market, or to put into service under its own name or trademark whether for payment, or free of charge.
Deployer	A natural or legal person, public authority, agency, or other body **using** an AI system under its authority.
Authorized representative	Any natural or legal person located or established in the EU who has received and accepted a written mandate from a provider to **carry out its obligations on its behalf.**
Importer	Any natural or legal person located or established in the EU that places on the market an AI system that bears the name or trademark of a natural or legal person established outside the EU.
Distributor	Any natural or legal person in the supply chain, **not being the provider or importer, who makes an AI system available in the EU market.**
Product manufacturer	A manufacturer of an AI system that is put on the market or a manufacturer that puts into service an AI system **together with its product** and under its own name or trademark.
Operator	A general term referring to all the terms above (provider, deployer, authorized representative, importer, distributor, or product manufacturer).

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 001061-24Gbl

ED None

BRIEFING

EU Legislation in Progress

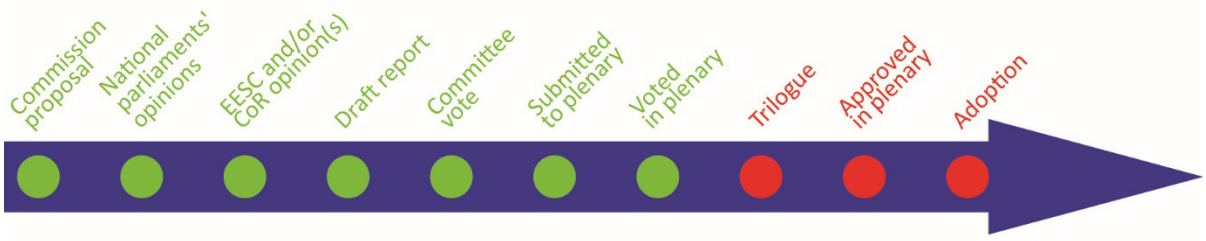
European Parliament

Artificial intelligence act

OVERVIEW

The European Commission tabled a proposal for an EU regulatory framework on artificial intelligence (AI) in April 2021. The draft AI act is the first ever attempt to enact a horizontal regulation for AI. The proposed legal framework focuses on the specific utilisation of AI systems and associated risks. The Commission proposes to establish a technology-neutral definition of AI systems in EU law and to lay down a classification for AI systems with different requirements and obligations tailored on a 'risk-based approach'. Some AI systems presenting 'unacceptable' risks would be prohibited. A wide range of 'high-risk' AI systems would be authorised, but subject to a set of requirements and obligations to gain access to the EU market. Those AI systems presenting only 'limited risk' would be subject to very light transparency obligations. The Council agreed the EU Member States' general position in December 2021. Parliament voted on its position in June 2023. EU lawmakers are now starting negotiations to finalise the new legislation, with substantial amendments to the Commission's proposal including revising the definition of AI systems, broadening the list of prohibited AI systems, and imposing obligations on general purpose AI and generative AI models such as ChatGPT.

Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts		
Committees responsible:	Internal Market and Consumer Protection (IMCO) and Civil Liberties, Justice and Home Affairs (LIBE) (jointly under Rule 58)	COM(2021)206 21.4.2021 2021/0106(COD)
Rapporteurs:	Brando Benifei (S&D, Italy) and Dragoş Tudorache (Renew, Romania)	
Shadow rapporteurs:	Deirdre Clune, Axel Voss (EPP); Petar Vitanov (S&D); Svenja Hahn, (Renew); Sergey Lagodinsky, Kim Van Sparrentak (Greens/EFA); Rob Rooken, Kosma Złotowski (ECR); Jean-Lin Lacapelle, Jaak Madison (ID); Cornelia Ernst, Kateřina Konecna (The Left)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Next steps expected:	Trilogue negotiations	



EPRS | European Parliamentary Research Service

Author: Tambiama Madiega; Graphic: Samy Chahri
Members' Research Service

PE 698.792 – June 2023

EN

Introduction

AI technologies are expected to bring a wide array of **economic and societal benefits** to a wide range of sectors, including environment and health, the public sector, finance, mobility, home affairs and agriculture. They are particularly useful for improving prediction, for optimising operations and resource allocation, and for personalising services.[1] However, the implications of AI systems for **fundamental rights** protected under the EU Charter of Fundamental Rights, as well as the **safety risks** for users when AI technologies are embedded in products and services, are raising concern. Most notably, AI systems may jeopardise fundamental rights such as the right to non-discrimination, freedom of expression, human dignity, personal data protection and privacy.[2]

Given the fast development of these technologies, in recent years AI regulation has become a central policy question in the European Union (EU). Policy-makers pledged to develop a **'human-centric' approach to AI** to ensure that Europeans can benefit from new technologies developed and functioning according to the EU's values and principles.[3] In its 2020 White Paper on Artificial Intelligence, the European Commission committed to **promote the uptake of AI** and **address the risks associated** with certain uses of this new technology. While the European Commission initially adopted a **soft-law approach**, with the publication of its non-binding 2019 Ethics Guidelines for Trustworthy AI and Policy and investment recommendations, it has since shifted towards a **legislative approach**, calling for the adoption of harmonised rules for the development, placing on the market and use of AI systems.[4]

AI regulatory approach in the world. While the United States of America (USA) had initially taken a lenient approach towards AI, calls for regulation have recently been mounting. The Cyberspace Administration of China is also consulting on a proposal to regulate AI, while the UK is working on a set of pro-innovation regulatory principles. At international level, the Organisation for Economic Co-operation and Development (OECD) adopted a (non-binding) Recommendation on AI in 2019, UNESCO adopted Recommendations on the Ethics of AI in 2021, and the Council of Europe is currently working on an international convention on AI. Furthermore, in the context of the newly established EU-US tech partnership (the Trade and Technology Council), the EU and USA are seeking to develop a mutual understanding on the principles underlining trustworthy and responsible AI. EU lawmakers issued a joint statement in May 2023 urging President Biden and European Commission President Ursula von der Leyen to convene a summit to find ways to control the development of advanced AI systems such as ChatGPT.

Parliament's starting position

Leading the EU-level debate, the European Parliament called on the European Commission to assess the impact of AI and to draft an EU framework for AI, in its wide-ranging 2017 recommendations on civil law rules on robotics. More recently, in 2020 and 2021, the Parliament adopted a number of non-legislative resolutions calling for EU action, as well as two legislative resolutions calling for the adoption of EU legislation in the field of AI. A first legislative resolution asked that the Commission establish a legal framework of ethical principles for the development, deployment and use of AI, robotics and related technologies in the Union. A second legislative resolution called for harmonisation of the legal framework for civil liability claims and imposition of a regime of strict liability on operators of high-risk AI systems. Furthermore, the Parliament adopted a series of recommendations calling for a common EU approach to AI in the intellectual property, criminal law, education, culture and audiovisual areas, and regarding civil and military AI uses.

Council starting position

In the past, the Council has repeatedly called for the adoption of common AI rules, including in 2017 and 2019. More recently, in 2020, the Council called upon the Commission to put forward concrete proposals that take existing legislation into account and follow a risk-based, proportionate and, if necessary, regulatory approach. Furthermore, the Council invited the EU and the Member States to

consider effective measures for identifying, predicting and responding to the potential impacts of digital technologies, including AI, on fundamental rights.

Preparation of the proposal

Following the White Paper on Artificial Intelligence[5] adopted in February 2020, the Commission launched a broad public consultation in 2020 and published an Impact Assessment of the regulation on artificial intelligence, a supporting study and a draft proposal, which received feedback from a variety of stakeholders.[6] In its impact assessment, the Commission identifies **several problems** raised by the development and use of AI systems, due to their specific characteristics.[7]

The changes the proposal would bring

The draft AI act has been designed as a **horizontal EU legislative instrument** applicable to all AI systems placed on the market or used in the Union.

Purpose, legal basis and scope

The **general objective** of the proposed AI act unveiled in April 2021 is to ensure the proper functioning of the single market by creating the conditions for the development and use of trustworthy AI systems in the Union. The draft sets out a harmonised legal framework for the development, placing on the Union market, and the use of AI products and services. In addition, the AI act proposal seeks to achieve a set of **specific objectives**: (i) ensure that AI systems placed on the EU market are safe and respect existing EU law, (ii) ensure legal certainty to facilitate investment and innovation in AI, (iii) enhance governance and effective enforcement of EU law on fundamental rights and safety requirements applicable to AI systems, and (iv) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.[8]

The new AI framework, based on Article 114[9] and Article 16[10] of the Treaty on the Functioning of the European Union (TFEU), would enshrine a **technology-neutral definition of AI systems** and adopt a **risk-based approach**, which lays down different **requirements and obligations** for the development, placing on the market and use of AI systems in the EU. In practice, the proposal defines common mandatory requirements applicable to the design and development of AI systems before they are placed on the market and harmonises the way ex-post controls are conducted. The proposed AI act would complement existing and forthcoming, horizontal and sectoral EU safety regulation.[11] The Commission proposes to follow the logic of the new legislative framework (NLF), i.e. the EU approach to ensuring a range of products comply with the applicable legislation when they are placed on the EU market through conformity assessments and the use of CE marking.

The new rules would apply primarily to **providers of AI systems established within the EU or in a third country** placing AI systems on the EU market or putting them into service in the EU, as well as to **users of AI systems located in the EU**.[12] To prevent circumvention of the regulation, the new rules would also apply to **providers and users of AI systems located in a third country** where the output produced by those systems is used in the EU.[13] However, the draft regulation does not apply to AI systems developed or used exclusively for military purposes, to public authorities in a third country, nor to international organisations, or authorities using AI systems in the framework of international agreements for law enforcement and judicial cooperation.

Definitions

No single definition of artificial intelligence is accepted by the scientific community and the term 'AI' is often used as a 'blanket term' for various computer applications based on different techniques, which exhibit capabilities commonly and currently associated with human intelligence.[14] The High Level Expert Group on AI proposed a baseline definition of AI that is increasingly used in the scientific literature, and the Joint Research Centre has established an operational definition of AI based on a taxonomy that maps all the AI subdomains from a political, research and industrial

perspective. However, the Commission found that the **notion of an AI system** should be more clearly defined, given that the determination of what an 'AI system' constitutes is crucial for the allocation of legal responsibilities under the new AI framework. The Commission therefore proposes to establish a legal definition of 'AI system' in EU law, which is largely based on a definition already used by the OECD.[15] Article 3(1) of the draft act states that '**artificial intelligence system**' means:

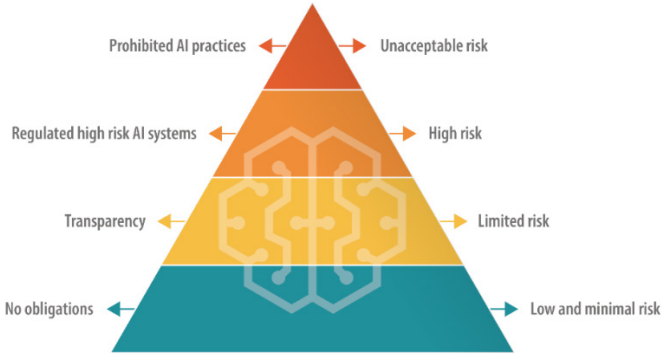
> *...software that is developed with [specific] techniques and approaches [listed in Annex 1] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.*[16]

Annex 1 of the proposal lays out a **list of techniques and approaches** that are used today to develop AI. Accordingly, the notion of 'AI system' would refer to a range of software-based technologies that encompasses '**machine learning**', '**logic and knowledge-based**' systems, and '**statistical**' approaches. This broad definition covers AI systems that can be used on a stand-alone basis or as a component of a product. Furthermore, the proposed legislation aims to be future-proof and cover current and future AI technological developments. To that end, the Commission would complement the Annex 1 list with new approaches and techniques used to develop AI systems as they emerge – through the adoption of **delegated acts** (Article 4).

Furthermore, Article 3 provides a long **list of definitions** including that of 'provider' and 'user' of AI systems (covering both public and private entities), as well as 'importer' and 'distributor', 'emotion recognition', and 'biometric categorisation'.

Risk-based approach

Pyramid of risks



Data source: European Commission.

The use of AI, with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour), can adversely affect a number of fundamental rights and users' safety. To address those concerns, the draft AI act follows a **risk-based approach** whereby legal intervention is tailored to concrete level of risk. To that end, the draft AI act distinguishes between AI systems posing (i) **unacceptable risk**, (ii) **high risk**, (iii) **limited risk**, and (iv) **low or minimal risk**. AI applications would be regulated only as strictly necessary to address specific levels of risk.[17]

Unacceptable risk: Prohibited AI practices

Title II (Article 5) of the proposed AI act explicitly **bans harmful AI practices** that are considered to be a clear threat to people's safety, livelihoods and rights, because of the 'unacceptable risk' they create. Accordingly, it would be prohibited to place on the market, put into services or use in the EU:

- AI systems that deploy harmful manipulative 'subliminal techniques';
- AI systems that exploit specific vulnerable groups (physical or mental disability);
- AI systems used by public authorities, or on their behalf, for social scoring purposes;
- 'Real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes, except in a limited number of cases.[18]

High risk: Regulated high-risk AI systems

Title III (Article 6) of the proposed AI act regulates 'high-risk' AI systems that create adverse impact on people's safety or their fundamental rights. The draft text distinguishes between two categories of high-risk AI systems.

- Systems used as a safety component of a product or falling under EU health and safety harmonisation legislation (e.g. toys, aviation, cars, medical devices, lifts).
- Systems deployed in **eight specific areas** identified in Annex III, which the Commission could update as necessary through **delegated acts** (Article 7):
  - Biometric identification and categorisation of natural persons;
  - Management and operation of critical infrastructure;
  - Education and vocational training;
  - Employment, worker management and access to self-employment;
  - Access to and enjoyment of essential private services and public services and benefits;
  - Law enforcement;
  - Migration, asylum and border control management;
  - Administration of justice and democratic processes.

All of these high-risk AI systems would be subject to a set of new rules including:

Requirement for an ex-ante conformity assessment: Providers of high-risk AI systems would be required to register their systems in an **EU-wide database** managed by the Commission before placing them on the market or putting them into service. Any AI products and services governed by existing product safety legislation will fall under the existing third-party conformity frameworks that already apply (e.g. for medical devices). Providers of AI systems not currently governed by EU legislation would have to conduct their own conformity assessment (**self-assessment**) showing that they comply with the new requirements and can use **CE marking**. Only high-risk AI systems used for biometric identification would require a conformity assessment by a 'notified body'.

Other requirements: Such high-risk AI systems would have to comply with a range of requirements particularly on risk management, testing, technical robustness, data training and data governance, transparency, human oversight, and cybersecurity (Articles 8 to 15). In this regard, providers, importers, distributors and users of high-risk AI systems would have to fulfil a range of obligations. Providers from outside the EU will require an **authorised representative** in the EU to (inter alia), ensure the conformity assessment, establish a post-market monitoring system and take corrective action as needed. AI systems that conform to the new **harmonised EU standards**, currently under development, would benefit from a presumption of conformity with the draft AI act requirements.[19]

Facial recognition: AI powers the use of biometric technologies, including facial recognition technologies (FRTs), which are used by private or public actors for verification, identification and categorisation purposes. In addition to the existing applicable legislation (e.g. data protection and non-discrimination), the draft AI act proposes to introduce new rules for FRTs and differentiate them according to their 'high-risk' or 'low-risk' usage characteristics. The use of real-time facial recognition systems in publicly accessible spaces for the purpose of law enforcement would be prohibited, unless Member States choose to authorise them for important public security reasons, and the appropriate judicial or administrative authorisations are granted. A wide range of FRTs used for purposes other than law enforcement (e.g. border control, market places, public transport and even schools) could be permitted, subject to a conformity assessment and compliance with safety requirements before entering the EU market.[20]

Limited risk: Transparency obligations

AI systems presenting 'limited risk', such as **systems that interacts with humans** (i.e. chatbots), **emotion recognition systems**, **biometric categorisation systems**, and AI systems that generate or manipulate image, audio or video content (i.e. **deepfakes**), would be subject to a limited set of transparency obligations.

Low or minimal risk: No obligations

All other AI systems presenting only low or minimal risk could be developed and used in the EU without conforming to any additional legal obligations. However, the proposed AI act envisages the creation of **codes of conduct** to encourage providers of non-high-risk AI systems to voluntarily apply the mandatory requirements for high-risk AI systems.

Governance, enforcement and sanctions

The proposal requires Member States to designate one or more competent authorities, including a **national supervisory authority**, which would be tasked with supervising the application and implementation of the regulation, and establishes a **European Artificial Intelligence Board** (composed of representatives from the Member States and the Commission) at EU level. National **market surveillance authorities** would be responsible for assessing operators' compliance with the obligations and requirements for high-risk AI systems. They would have access to confidential information (including the source code of the AI systems) and subject to binding confidentiality obligations. Furthermore, they would be required to take any **corrective measures** to prohibit, restrict, withdraw or recall AI systems that do not comply with the AI act, or that, although compliant, present a risk to health or safety of persons or to fundamental rights or other public interest protection. In case of persistent non-compliance, Member States will have to take all appropriate measures to restrict, prohibit, recall or withdraw the high-risk AI system at stake from the market.

Administrative **fines** of varying scales (up to €30 million or 6 % of the total worldwide annual turnover), depending on the severity of the infringement, are set as sanctions for non-compliance with the AI act. Member States would need to lay down rules on penalties, including administrative fines and take all measures necessary to ensure that they are properly and effectively enforced.

Measures to support innovation

The Commission proposes that Member States, or the European Data Protection Supervisor, could establish a **regulatory sandbox**, i.e. a controlled environment that facilitates the development, testing and validation of innovative AI systems (for a limited period of time) before they are put on the market. Sandboxing will enable participants to use personal data to foster AI innovation, without prejudice to the GDPR requirements. Other measures are tailored specifically to small-scale providers and **start-ups**

Advisory committees

The European Economic and Social Committee adopted its opinion on the proposed artificial intelligence act on 22 September 2021.

National parliaments

The deadline for the submission of reasoned opinions on the grounds of subsidiarity was 2 September 2021. Contributions were received from the Czech Chamber of Deputies and the Czech Senate, the Portuguese Parliament, the Polish Senate and the German Bundesrat.

Stakeholder views[21]

Definitions

Definitions are a contentious point of discussion among stakeholders. The Big Data Value Association, an industry-driven international not–for-profit organisation, stresses that the definition of AI systems is quite broad and would cover far more than what is subjectively understood as AI, including the simplest search, sorting and routing algorithms, which would consequently be subject to new rules. Furthermore, they ask for clarification of how components of larger AI systems (such

as pre-trained AI components from other manufacturers or components not released separately), should be treated. AmCham, the American Chamber of Commerce in the EU, suggests avoiding over-regulation by adopting a narrower definition of AI systems, focusing strictly on high-risk AI applications (and not extended to AI applications that are not high-risk, or software in general). AccessNow, an association defending users' digital rights argues the definitions of 'emotion recognition' and 'biometric categorisation' are technically flawed, and recommends adjustments.

Risk-based approach

While they generally welcome the proposed AI act's risk-based approach, some stakeholders support wider prohibition and regulation of AI systems. Civil rights organisations call for a ban on indiscriminate or arbitrarily targeted use of biometrics in public or publicly accessible spaces, and for restrictions on the uses of AI systems, including for border control and predictive policing. AccessNow argues that the provisions concerning prohibited AI practices (Article 5) are too vague, and proposes a wider ban on the use of AI to categorise people based on physiological, behavioural or biometric data, for emotion recognition, as well as dangerous uses in the context of policing, migration, asylum, and border management. Furthermore, they call for stronger impact assessment and transparency requirements.

The European Enterprises Alliance stresses that there is general uncertainty about the roles and responsibilities of the different actors in the AI value chain (developers, providers, and users of AI systems). This is particularly challenging for companies providing general purpose application programming interfaces or open-source AI models that are not specifically intended for high-risk AI systems but are nevertheless used by third parties in a manner that could be considered high-risk. They also call for 'high-risk' to be redefined, based on the measurable harm and potential impact. AlgorithmWatch underlines that the applicability of specific rules should not depend on the type of technology, but on the impact it has on individuals and society. They call for the new rules to be defined according to the impact of the AI systems and recommend that every operator should conduct an impact assessment that assesses the system's risk levels on a case-by-case basis. Climate Change AI calls for climate change mitigation and adaptation to be taken into account in the classification rules for high-risk AI systems and impose environmental protection requirements.

Consumer protection

The European Consumer Organisation, BEUC, stresses that the proposal requires substantial improvement to guarantee consumer protection. The organisation argues that the proposal should have a broader scope and impose basic principles and obligations (e.g. on fairness, accountability and transparency) upon all AI systems, as well as prohibiting more comprehensively harmful practices (such as private entities' use of social scoring and of remote biometric identification systems in public spaces). Furthermore, consumers should be granted a strong set of rights, effective remedies and redress mechanisms, including collective redress.

Impact on investments and SMEs

There are opposing views on the impact of the proposed regulation on investment. A study by the Centre for Data Innovation (representing large online platforms) highlights that the compliance costs incurred under the proposed AI act would likely provoke a chilling effect on investment in AI in Europe, and could particularly deter small and medium-sized enterprises (SMEs) from developing high-risk AI systems. According to the Centre for Data Innovation, the AI act would cost the European economy €31 billion over the next five years and reduce AI investments by almost 20 %. However, such estimates of the compliance costs are challenged by the experts from the Centre for European Policy Studies, as well as by other economists. The European Digital SME Alliance warns against overly stringent conformity requirements, asks for effective representation of SMEs in the standards-setting procedures and for making sandboxes mandatory in all EU Member States.

Academic and other views

While generally supporting the Commission's proposal, critics call for amendments, including revising the 'AI systems' definition, ensuring a better allocation of responsibility, strengthening enforcement mechanisms and fostering democratic participation.[22] Among the main issues are:

AI systems definition

The legal definition of 'AI systems' contained in the proposed AI act has been heavily criticised. Smuha and others warn the definition lacks clarity and may lead to legal uncertainty, especially for some systems that would not qualify as AI systems under the draft text, while their use may have an adverse impact on fundamental rights.[23] To address this issue, the authors propose to **broaden the scope of the legislation** to explicitly include all computational systems used in the identified high-risk domains, regardless of whether they are considered to be AI. According to the authors, the advantage would be in making application of the new rules more dependent on the domain in which the technology is used and the fundamental rights-related risks, rather than on a specific computational technique. Ebers and others consider that the scope of 'AI systems' is overly broad, which may lead to **legal uncertainty** for developers, operators, and users of AI systems and ultimately to over-regulation.[24] They call on EU law-makers to exempt AI systems developed and used for **research purposes** and **open-source software** (OSS) from regulation. Other commentators question whether the proposed definition of 'AI systems' is truly **technology neutral** as it refers primarily to 'software', omitting potential future AI developments.

Risk-based approach

Academics also call for amendments, warning that the risk-based approach proposed by the Commission would not ensure a high level of protection of fundamental rights. Smuha and others argue that the proposal does not always accurately recognise the wrongs and harms associated with different kinds of AI systems and therefore does not appropriately allocate responsibility. Among other things, they recommend adding a procedure that enables the Commission to **broaden the list of prohibited AI systems**, and propose banning existing manipulative AI systems (e.g. deepfakes), social scoring and some biometrics. Ebers and others call for a **more detailed classification of risks** to facilitate industry self-assessment and support, as well as **prohibiting more AI systems** (e.g. biometrics), including in the context of **private use**. Furthermore, some highlight that the draft legislation does not address **systemic sustainability risks** created by AI especially in the area of climate and environmental protection.[25]

Experts seem particularly concerned by the implementation of Article 5 (prohibited practices) and Article 6 (regulated high-risk practices). One of the major concerns raised is that the rules on prohibited and high-risk practices may prove ineffective in practice, because the risk assessment is left to provider **self-assessment**. Veale and Zuiderveen Borgesius warn that most providers can arbitrarily classify most high-risk systems as adhering to the rules using self-assessment procedures alone. Smuha and others recommend exploring whether certain high-risk systems would not benefit from a conformity assessment carried out by an **independent entity** prior to their deployment.

Biometrics regulation. A study commissioned by the European Parliament recommends, inter alia, to empower the Commission to adapt the list of prohibited AI practices periodically, under the supervision of the European Parliament, and the adoption of a more comprehensive list of 'restricted AI applications' (comprising real-time remote biometric identification without limitation for law enforcement purposes). Regulation of facial recognition technologies (FRTs) is one of the most contentious issues.[26] The European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) have called for a general ban on any uses of AI for the automated recognition of human features in publicly accessible spaces.

Governance structure and enforcement and redress mechanisms

Ebers and others stress that the AI act **lacks effective enforcement structures**, as the Commission proposes to leave the preliminary risk assessment, including the qualification as high-risk, to the providers' self-assessment. They also raise concerns about the excessive delegation of regulatory power to private European standardisation organisations (ESOs), due to the lack of democratic oversight, the impossibility for stakeholders (civil society organisations, consumer associations) to influence the development of standards, and the lack of judicial means to control them once they have been adopted. Instead, they recommend that the AI act codifies a set of legally binding requirements for high-risk AI systems (e.g. prohibited forms of algorithmic discrimination), which ESOs may specify through harmonised standards. Furthermore, they advocate that European policy-makers should **strengthen democratic oversight of the standardisation process**.

Commentators deplore a crucial gap in the AI act, which does not provide for **individual enforcement rights**. Ebers and others stress that individuals affected by AI systems and civil rights organisations have no **right to complain** to market surveillance authorities or to sue a provider or user for failure to comply with the requirements. Similarly, Veale and Zuiderveen Borgesius warn that, while some provisions of the draft legislation aim to impose obligations on AI systems users, there is **no mechanism for complaint or judicial redress** available to them. Smuha and others recommend amending the proposal to include, inter alia, an **explicit right of redress for individuals** and **rights of consultation and participation for EU citizens** regarding the decision to amend the list of high-risk systems in Annex III.

It has also been stressed that the text as it stands **lacks proper coordination** mechanisms between authorities, in particular concerning **cross-border infringement**. Consequently, the competence of the relevant authorities at national level should be clarified. Furthermore, guidance would be desirable on how to ensure compliance with transparency and information requirements, while simultaneously **protecting intellectual property rights and trade secrets** (e.g. to what extent the source code must be disclosed), not least to avoid diverging practices in the Member States.

Legislative process

The **Council** adopted its common position in December 2022. The Council's proposes, inter alia to:

- narrow the definition of AI systems to systems developed through machine learning approaches and logic- and knowledge-based approaches;
- extend to private actors the prohibition on using AI for social scoring, and add cases when the use of 'real-time' remote biometric identification systems in publicly accessible spaces could exceptionally be allowed;
- impose requirements on general purpose AI systems by means of implementing acts;
- add new provisions to take into account situations where AI systems can be used for many different purposes (general purpose AI); and
- simplify the compliance framework for the AI Act and strengthen, in particular, the role of the AI Board.

In **Parliament**, the file was assigned jointly (under Rule 58) to the Committee on Internal Market and Consumer Protection (IMCO) and the Committee on Civil Liberties, Justice and Home Affairs (LIBE), with Brando Benifei (S&D, Italy) and Dragos Tudorache, Renew, Romania) appointed as rapporteurs. In addition, the Legal Affairs Committee (JURI), the Committee on Industry, Research and Energy (ITRE) and the Committee on Culture and Education (CULT) are each associated to the legislative work under Rule 57, with shared and/or exclusive competences for specific aspects of the proposal. Parliament adopted its negotiating position (499 votes in favour, 28 against and 93 abstentions) on 14 June 2023, with substantial amendments to the Commission's text, including:

- **Definitions**. Parliament amended the definition of AI systems to align it with the definition agreed by the OECD. Furthermore, Parliament enshrines a definition of

'general purpose AI system' and 'foundation model' in EU law.

- **Prohibited practices**. Parliament substantially amended the list of AI systems prohibited in the EU. Parliament wants to ban the use of biometric identification systems in the EU for both real-time and ex-post use (except in cases of severe crime and pre-judicial authorisation for ex-post use) and not only for real-time use, as proposed by the Commission. Furthermore, Parliament wants to ban all biometric categorisation systems using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation); predictive policing systems (based on profiling, location or past criminal behaviour); emotion recognition systems (used in law enforcement, border management, workplace, and educational institutions); and AI systems using indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases.
- **High-risk AI systems**. While the Commission proposed to automatically categorise as high-risk all systems in certain areas or use cases, Parliament adds the additional requirement that the systems must pose a 'significant risk' to qualify as high-risk. AI systems that risk harming people's health, safety, fundamental rights or the environment would be considered as falling within high-risk areas. In addition, AI systems used to influence voters in political campaigns and AI systems used in recommender systems displayed by social media platforms, designated as very large online platforms under the Digital Services Act, would be considered high-risk systems. Furthermore, Parliament imposes on those deploying a high-risk system in the EU an obligation to carry out a fundamental rights impact assessment.
- **General-purpose AI, generative AI and foundation models.** Parliament sets a layered regulation of general-purpose AI. Parliament imposes an obligation on providers of foundation models to ensure robust protection of fundamental rights, health, safety, the environment, democracy and the rule of law. They would be required to assess and mitigate the risks their models entail, comply with some design, information and environmental requirements and register such models in an EU database. Furthermore, generative foundation AI models (such as ChatGPT) that use large language models (LLMs) to generate art, music and other content would be subject to stringent transparency obligations. Providers of such models and of generative content would have to disclose that the content was generated by AI not by humans, train and design their models to prevent generation of illegal content and publish information on the use of training data protected under copyright law. Finally, all foundation models should provide all necessary information for downstream providers to be able to comply with their obligations under the AI act.
- **Governance and enforcement**. National authorities' competences would be strengthened, as Parliament gives them the power to request access to both the trained and training models of the AI systems, including foundation models. Parliament also proposes to establish an AI Office, a new EU body to support the harmonised application of the AI act, provide guidance and coordinate joint cross-border investigations. In addition, Members seek to strengthen citizens' rights to file complaints about AI systems and receive explanations of decisions based on high-risk AI systems that significantly impact their rights.
- **Research and innovation**. To support innovation, Parliament agrees that research activities and the development of free and open-source AI components would be largely exempted from compliance with the AI act rules.