The European Union Artificial Intelligence Act

Latest developments and key takeaways

2 February 2024

EY

Building a better
working world

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.

Contacts

For questions about AI public policy and regulation:

Shawn Maher
EY Global Vice Chair, Public Policy
shawn.maher@eyg.ey.com

Ansgar Koene
EY Global AI Ethics and Regulatory Leader
ansgar.koene1@be.ey.com

Anne McCormick
EY EMEIA Digital Policy Leader
anne.mccormick@uk.ey.com

Andrew Hobbs
EY EMEIA Public Policy Leader
ahobbs@uk.ey.com

John Hallmark
EY Americas Public Policy
EY US Political and Legislative Leader
Ernst and Young LLP
john.hallmark@ey.com
Yi Xie
EY Asia-Pacific Public Policy
yi.y.xie@hk.ey.com

Dean Protheroe
EY EMEIA Public Policy
dprotheroe@uk.ey.com

For questions about AI:

Nicola Morini Bianzino
EY Global Chief Technology Officer
nicola.morini.bianzino@eyg.ey.com

Beatriz Saiz-Sanz
EY Global Data and AI Leader
beatriz.sanzsaiz@es.ey.com

Jay Persaud
EY Global Emerging Technologies Ecosystem Leader
jay.persaud@ey.com

Richard Jackson
EY Global AI Assurance Leader
richard.jackson@ey.com

Dan Diasio
EY Global AI Consulting Leader
dan.diasio@ey.com

Frank de Jonghe
EY EMEIA Trusted AI Leader
frank.de.jonghe1@uk.ey.com

Peter Katko
EY Global Digital Law Leader
peter.katko@de.ey.com

Contents

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.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

EYG no. 001061-24Gbl

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com