Anthology
power of together

Navigating the EU AI Act

Authors: Stephan Geering, Deputy General Counsel & Compliance, Trustworthy AI and Global Privacy Officer at Anthology; Juan Medina, Corporate Counsel, Anthology

Table of Contents

1. Introduction

The European Union Artificial Intelligence Act (EU AI Act) represents a pioneering effort to regulate artificial intelligence comprehensively within the EU. It introduces a product safety-oriented and risk-based framework, categorizing AI systems by their potential risks to safety and fundamental rights and applying corresponding obligations to providers, deployers, and other users of AI systems. Anthology welcomes the EU AI Act. The lawful, ethical, and responsible use of AI is a key priority for Anthology. We are implementing the EU AI Act by building on our established **Trustworthy AI Program** and principles. This white paper aims to provide a high-level overview of the EU AI Act and explain our implementation approach.

2. Overview of the EU AI Act

2.1 Scope of the EU AI ACT

The EU AI Act applies to both public and private sector entities that market, use, or provide AI-related services within the EU. It covers all AI systems that fall within the defined risk categories and that operate within the EU, regardless of whether the provider or deployer is located inside or outside the EU (as long as the output of the AI system is intended to be used in the EU).

The EU AI Act also ensures application across the whole supply chain. While most obligations apply to providers and deployers, importers and distributors of AI systems also need to meet certain obligations (see section 2.3 for the definition of these roles).

2.2 Key Objectives of the EU AI Act

- **Protecting fundamental rights** such as privacy, non-discrimination, and freedom of expression.
- **Promoting transparency and accountability** by requiring providers to disclose information about the capabilities and limitations of their AI systems.
- **Fostering innovation** by providing clear legal guidelines and encouraging the development of AI systems that are safe, ethical, and aligned with societal values.
- **Harmonising standards** by ensuring that AI systems developed in one member state can be deployed across the EU without facing regulatory barriers.

2.3 Key Definitions

The EU AI Act is based on EU product safety laws. It therefore uses product safety definitions and concepts. Particularly noteworthy is that the definition for “AI Systems” is very broadly defined. It is also intentionally similar to the definitions of the OECD and NIST.

- **AI system:** A machine-based system that is 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.
- **General-purpose AI model:** AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing 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, except AI models that are used for research, development, or prototyping activities before they are placed on the market.
- **Provider:** Develops an AI system or a general-purpose AI model or has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark.
- **Deployer:** Uses an AI system under its authority. A deployer can be a natural or legal person, public authority, agency, or other body. EU institutions, bodies, offices, and agencies may also act as a deployer.
- **Importer:** Natural or legal person located or established in the EU that places an AI system bearing the name or trademark of a person not established in the EU on the EU market.
- **Distributor:** Natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market.

2.4 EU AI Act Timeline

The EU AI Act entered into force on 1 August 2024. The key implementation date is 2 August 2026 but there are some obligations that apply earlier and some that apply later (see table below).

Date	Applicable requirements
2 February 2025	Prohibited practices ban AI literacy requirements
2 August 2025	Obligations for general-purpose AI models Supervision and enforcement governance and penalties (other than in relation to general-purpose AI models)
2 August 2026	All other provisions of the EU AI Act (except for those below)
2 August 2027	Requirements for high-risk categories listed in Annex I General-purpose AI models placed on the market before 2 August 2025
2 August 2030	High-risk AI systems (other than those listed below), which have been placed on the market or put into service before 2 August 2026 and which are intended to be used by public authorities
31 December 2030	Components of large-scale IT systems listed in Annex X, which have been placed on the market or put into service before 2 August 2027 and are intended to be used by public authorities

2.5 Supervision and Enforcement

The EU AI Act uses a complex and multi-level supervision model[1]. On the EU-level, the European Artificial Intelligence Office (the AI Office) plays a key role as the central authority on AI expertise and implementation of the legal framework. But every EU Member State will also appoint supervision and market surveillance authorities. While the AI Office will be the main regulator for general-purpose AI models, the national authorities will oversee the regulated AI systems.

The EU AI Act defined the overarching legal framework. It will be complemented by an array of regulatory documentation both on the EU and Member State level. The AI Office and Member State authorities will issue critical guidance. Also, EU standardisation bodies like CEN and CENELEC are tasked with publishing harmonised standards with detailed technical requirements for providers and deployers of high-risk AI systems. Industry stakeholders can draft and adhere to codes of practice and codes of conduct. Such codes may be adopted as generally valid by the European Commission.

With regard to enforcement, the EU AI Act includes significant penalties for non-compliance[2] which depend on the nature of the violation and the size of the organization:

- Non-compliance with the rules on prohibited practices: EUR 35 million or 7% of the total worldwide annual turnover, whichever is higher
- Non-compliance relating to obligations for regulated AI systems and/or general-purpose AI models: up to EUR 15 million or up to 3% of the total worldwide annual turnover, whichever is higher
- Supplying incorrect, incomplete, or misleading information to authorities in reply to a request: up to EUR 7.5 million or up to 1% of the total worldwide annual turnover, whichever is higher

3. Risk-Based Classification of AI Systems

3.1 The Four Risk Categories

The EU AI Act classifies AI systems based on their risk to individuals and society, with high-risk AI systems facing the most stringent requirements.

The four risk categories defined by the Act are as follows:

- **Unacceptable risk (prohibited):** AI systems that pose an unacceptable risk to safety or rights (e.g., social scoring, behavioural manipulation, biometric categorization systems using sensitive characteristics).
- **High risk (significant obligations):** Certain AI systems that pose a significant risk of harm to health, safety, or fundamental rights (e.g., certain systems related to employment and worker management, education and vocational training, essential services and benefits) (see section 3.2 below).
- **Limited risk (limited obligations):** AI systems where a lack of transparency introduces risk (e.g., chatbots).
- **Minimal risk (no obligations[3]):** AI systems that do not fall into the three categories above (e.g., AI-enabled video games or spam filters).

1 See Future of Privacy Forum's EU AI Act governance chart **here**
2 Article 99
3 The best effort obligation to ensure AI literacy in Article 4 applies (see section 4.1 below)

3.2 High-Risk AI Systems in Education

AI systems used for certain education-related activities are classified as high-risk under the EU AI Act[4] due to the considerable influence that AI systems can have on the fundamental rights of individuals and their access to educational opportunities. This classification can impact both education technology providers such as Anthology as well as educational institutions. The categories of high-risk activities are broadly defined. The following four categories of AI systems are considered high-risk:

AI systems intended to be used in the context of educational and vocational training institutions …

1. *To **determine access or admission** or to assign individuals to educational and vocational training institutions;*
2. *To **evaluate learning outcomes**, including when those outcomes are used to steer the learning process of individuals;*
3. *For the purpose of **assessing the appropriate level of education** that an individual will receive or will be able to access;*
4. *For monitoring and detecting prohibited behaviour of students during tests **(proctoring)**.*

To reduce the impact of the broad scope, AI systems from the above four categories are excluded if they do not pose a significant risk of harm to the health, safety, or fundamental rights of individuals[5]. As such, AI systems from the four categories above are not considered high-risk if they do not perform profiling and are intended for:

- Performing a narrow procedural task (e.g., transforming unstructured data into structured data, detection of duplication)
- Improving the result of a previously completed human activity (e.g., improving the tone or style of language in documents)
- Detecting decision-making patterns or deviations from prior decision-making patterns when not meant to replace or influence the previously completed human assessment, without proper human review (e.g., flagging grading inconsistencies compared with an existing grading pattern for that instructor)
- Performing a preparatory task to an assessment relevant for the purpose of the four high-risk categories (e.g., transcribing or translating documents)

The EU Commission is tasked to provide guidance on the classification of high-risk AI systems, but this guidance is only due 2 February 2026 (i.e., six months before the EU AI Act obligations for high-risk AI systems come into effect).

As part of its EU AI Act implementation (see section 5 below), Anthology is reviewing all of its AI-powered product features to determine whether any features need to be considered high-risk AI systems.

4. Key Obligations

4 Article 6(2) in combination with Annex III
5 Article 6(3)

4.1 All AI Systems: AI Literacy

The AI literacy rules apply to all providers and deployers of AI systems. While the EU AI Act does not specify in detail what is required for AI literacy, providers and deployers need to make best efforts to ensure their staff, and other persons dealing with the operation and use of AI systems on their behalf, have a sufficient level of knowledge, skills, and understanding regarding the deployment of AI systems, their opportunities, and risks.

4.2 Limited-Risk AI Systems: Transparency

The EU AI Act includes transparency obligations for limited-risk AI systems with the following characteristics[6]:

- Designed to interact directly with individuals
- Generate synthetic audio, image, video, or text content, including deepfakes
- Emotion recognition or biometric categorisation systems

Transparency obligations for limited-risk AI systems apply to both providers and/or deployers, depending on the category of system. For example, the EU AI Act includes obligations for providers to label AI-generated or manipulated outputs and for deployers to be transparent about their use of deepfakes.

4.3 High-Risk AI Systems: Provider Obligations

It's important to note that an importer, distributor, deployer, or any other party can become a provider under certain circumstances, which means that the full list of provider obligations apply[7]. Importers, distributors, or deployers will be considered a provider of a high-risk AI system if they have put their name or trademark on the system or if they make substantial modifications to or modify the intended purpose of the AI system, which renders the system high-risk.

For providers of AI systems deemed high-risk, the regulation imposes stringent obligations such as:

- Ensuring their AI systems meet the requirements and are able to demonstrate the AI systems' compliance
- Risk management and data governance frameworks
- Establishing a sound quality management system
- Maintaining detailed technical documentation
- Supporting deployers with documentation and instructions
- Ensuring or enabling human oversight for high-risk AI systems
- Implementing the necessary accuracy, robustness, and security measures
- Ensuring the AI systems undergo the appropriate conformity assessment, draw up an EU declaration of conformity, and affix a CE marking to the system
- Registering the system in the EU database of high-risk systems
- Meeting accessibility requirements
- Implementing post-market monitoring

6 Art. 50
7 Art. 25(1)

- Reporting of serious incidents
- Taking the necessary corrective actions, including withdrawing the system or disabling it if it is not/no longer in conformity

4.4 High-Risk AI Systems: Deployer Obligations

The EU AI Act also imposes obligations on deployers of high-risk AI systems, including the following key obligations:

- Implementing appropriate technical and organizational measures to ensure the AI systems are used in line with the instructions of the provider
- Ensuring that human oversight is performed by individuals with the necessary competence and support
- Ensuring input data is relevant and representative (to the extent the deployer has control over the input data)
- Monitoring the AI system's operation and reporting any risks and incidents to the provider, importer, distributor, and authorities
- Conducting a data protection impact assessment and fundamental rights impact assessment where necessary
- Deployers of high-risk AI systems who are public authorities, or Union institutions, bodies, offices, or agencies must comply with the EU Database registration obligations[8]
- Informing employees and employee representatives before implementing a high-risk AI system in the workplace
- Informing persons that are subject to the use of a high-risk AI system when making use of the AI system to make decisions or assist in making decisions with respect to these persons

4.5 Requirements for General-Purpose AI Models

The EU AI Act generally regulates AI systems, not models. However, in the light of the advent of powerful large language models like OpenAI's GPT models and Google's Gemini models, the EU included additional rules on general-purpose AI models which apply when such a model is made available or put into service on the EU market, including in the scenario that the provider of a general-purpose AI model integrates its model into its own AI system.

Additionally, obligations for general-purpose AI models apply to third parties which fine-tune or modify such models.[9]

5. Anthology's Implementation of the EU AI Act

5.1 Our Trustworthy AI Approach

The lawful, ethical, and responsible use of AI is a key priority for Anthology. While the EU AI Act and the rise of sophisticated generative AI models have brought more attention to AI risks, such risks are not new. And they are not new to us. Anthology has been actively thinking about AI risk management for years: In 2018 we brought institutions and academics together to discuss **Ethical AI in Higher Education**. In 2023 we formally implemented a **Trustworthy AI Program**, which is led by our Trustworthy AI Officer.

5.2 Our Trustworthy AI Principles

Our Trustworthy AI program commits Anthology to implementing the following principles. These principles are based on and aligned to the principles of the **NIST AI Risk Management Framework,** the **EU AI Act**, and the **OECD AI**

8 Article 49
9 Recital 109

Principles. The principles apply to both our internal use of AI as well as to AI functionalities in products we provide to our customers.

- **Fairness:** Minimizing harmful bias in AI systems
- **Reliability:** Taking measures to ensure the output of AI systems is valid and reliable
- **Humans in Control:** Ensuring humans ultimately make decisions that have legal or otherwise significant impact
- **Transparency and Explainability:** Explaining to users when AI systems are used, how the AI systems work, and helping users interpret and appropriately use the output of the AI systems
- **Privacy, Security, and Safety:** AI systems should be secure, safe, and privacy friendly
- **Value alignment:** AI systems should be aligned to human values, in particular those of our customers and users
- **Accountability:** Ensuring there is clear accountability regarding the trustworthy use of AI systems within Anthology as well as between Anthology, its customers, and its providers of AI systems/models

5.3 Our Trustworthy AI Principles

Our Trustworthy AI program is aligned to the NIST AI Risk Management Framework and the requirements of the EU AI Act. The program builds on and integrates with our ISO-certified data privacy and security risk management programs and processes.

- **Governance:** A cross-functional Trustworthy AI Council oversees and advances the program, and we leverage our existing ISO-certified data privacy and security risk management processes
- **Policy:** Our internal Trustworthy AI Policy documents the above principles and our approach to governance and risk management
- **Training and awareness:** Our employees undergo annual ethical AI training, and we use regular communications to raise employee awareness
- **Inventory of AI systems:** We established inventories to track and manage the use of AI systems in our corporate infrastructure and our products
- **Product requirements and reviews:** We are using defined product requirements and formalised reviews, leveraging our established data privacy and security review processes

5.4 EU AI Act Implementation Program

A key priority of the Trustworthy AI Program and team for 2025 and beyond is the implementation of, and ongoing compliance with, the EU AI Act, as well as supporting our customers with their obligations under the EU AI Act. Our implementation project has the following key components:

- **Dedicated EU AI implementation project:** Anthology's Legal team has established a dedicated implementation project that will oversee and coordinate the implementation efforts under the supervision of the Trustworthy AI Council
- **Updating Trustworthy AI program and governance:** We will review our Trustworthy AI program and governance structures to determine when enhancements are required to meet the EU AI Act obligations and update the program as necessary
- **Inventory and classification of AI systems:** We are leveraging our existing inventories to create a detailed inventory system that allows for the EU AI Act risk classification (unacceptable risk, high risk, limited risk, or minimal risk)

- **Implementing the necessary systems and processes for high-risk AI systems:** For AI systems identified as high-risk, Anthology will implement the necessary programs and controls, including setting up quality management and risk management systems, conducting conformity assessments, and developing the necessary documentation to support our customers as the deployers of the AI high-risk systems
- **Implementing transparency measures for limited-risk systems:** For AI systems classified as limited-risk, Anthology will review its existing transparency documentation and implement any necessary enhancements
- **Promoting AI literacy across the organization:** Anthology will further build out its existing AI literacy efforts (including our ethical AI training) to add more targeted and role-based training and to otherwise meet the AI literacy requirements
- **Joining the EU AI Pact:** Anthology is a participant of the EU's **AI Pact** initiative; as part of that participation, Anthology pledges to (continue to) adopt an AI governance strategy and work towards EU AI Act implementation, identify high-risk AI systems, and promote AI literacy

6. Five Steps to Help Prepare for the EU AI Act

1. **Build and maintain a Trustworthy AI Program:** Organisations that already have a trustworthy AI[10] program have a considerable advantage. They can leverage their existing program for the EU AI Act implementation and build on it. Organisations that have not fully implemented such a program yet should accelerate their efforts. Helpful guidance on how to implement a program and policy framework can be found in our **AI Policy Framework** document. Following a cross-functional approach and obtaining executive-level backing are crucial for a successful program.
2. **Identify, inventory, and classify AI systems:** A critical step is to work across the organisation with IT, Procurement, HR, and other departments to identify where AI systems are being used. Once inventoried, the AI systems need to be assessed to determine in which EU AI Act risk category they may fall.
3. **Gap assessment and action plans:** Once the AI systems have been categorised, the next step is to determine which additional steps are required for the regulated categories of AI systems and to develop the necessary action plans. To that end, it is essential to understand the role of the organisation (e.g., deployer) under the EU AI Act.
4. **Update vendor risk management processes:** For many organisations, third-party applications will be the main source of AI systems. Organisations should therefore update their vendor due diligence and risk management processes to identify, assess, and manage the risks related to third-party AI systems.
5. **Follow regulatory developments closely:** As mentioned in section 2.5 above, the EU AI Act will be complemented by a raft of guidelines and technical standards. These can have a significant impact on compliance obligations. It is therefore essential there is a clearly assigned team (e.g., the legal department) that tracks these developments and can provide internal guidance on how they impact internal program and action plans.

10 Sometimes also called "responsible AI" or "ethical AI"

7. Helpful Resources

Official EU resources:

- Official text of the EU AI Act: **EU AI Act - Full Text**
- EU Commission website for the AI Act: **https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai**
- AI Office website: **https://digital-strategy.ec.europa.eu/en/policies/ai-office**
- AI Pact website: **https://digital-strategy.ec.europa.eu/en/policies/ai-pact**

Anthology resources:

- **Trustworthy AI Approach** (statement on our approach)
- **Generative AI features** (list of our generative AI features with links to detailed transparency notes)
- **AI Policy Framework** (recommendations for customers on how to implement a responsible AI framework)
- **Data Privacy Approach**
- **Data Privacy White Paper** (PDF)
- **Product Security**
- **Our privacy and security certifications**

Official EU resources:

- **The William Fry AI Guide**
- **EU AI Act - A Pioneering Legal Framework On Artificial Intelligence - Practical Guide** (Cuatrecasas)
- **Decoding the EU Artificial Intelligence Act** (KPMG)
- **EU AI Act: Navigating a Brave New World** (Latham & Watkins)
- **Conformity Assessments Under the Proposed EU AI Act: A Step-By-Step Guide** (Future of Privacy Forum & OneTrust)
- **European Union Artificial Intelligence Act Guide** (Bird & Bird)
- **FPF's AI Governance framework chart**

Disclaimer: *These materials have been prepared solely for informational purposes and should not be considered legal advice. This white paper is up-to-date as of the date of publication. Please visit our* ***Trust Center*** *for the latest version.*