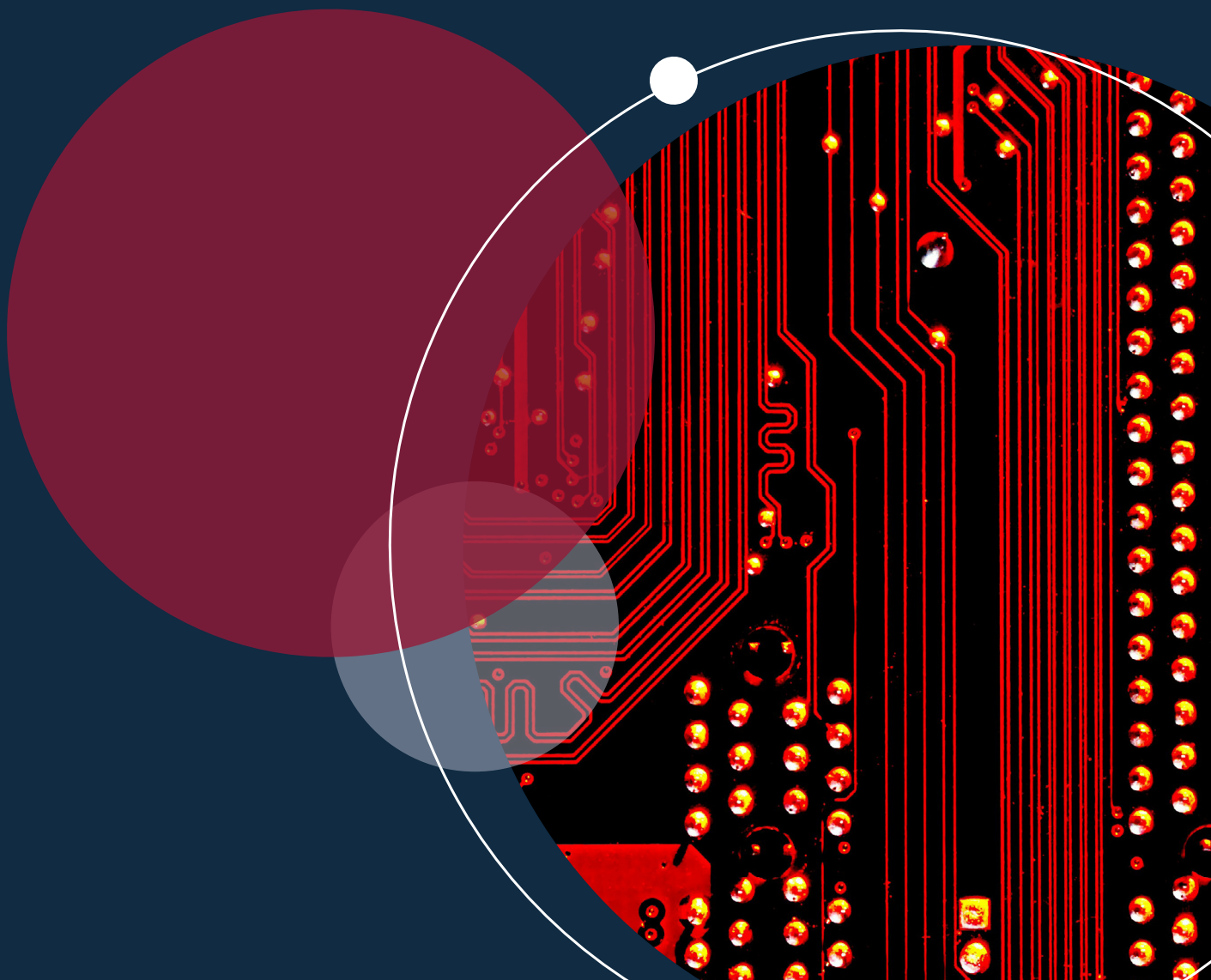


Step toe

# EU AI Act Decoded



## Which AI systems and models will be subject to the EU AI Act?

The EU AI Act will apply to:

- **“AI systems”**: “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”.

### Autonomy

A system that has some degree of independence of actions from human involvement and of capabilities to operate without human intervention.

### Adaptiveness after deployment

A system that demonstrates self-learning capabilities, allowing the system to change while in use.

### Infers, from the input it receives, how to generate outputs

A key characteristic of AI system, this refers to the process of obtaining outputs which can influence the environments, and to a capability of deriving models or algorithms, or both, **from inputs**. It goes **beyond basic data processing** and can be enabled through techniques such as machine learning and logic-and knowledge-based approaches.

### Notes

- This definition is **largely inspired from the OECD’s** definition of AI system;
- It aims to be **technology-neutral** and **innovation-proof**;
- It aims at **distinguishing AI systems from simpler traditional software systems or programming approaches**, and does not cover systems that are based on the rules defined solely by natural persons to automatically execute operations.



- **“General-purpose AI models”**: “An **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”.\*

### AI model

Although AI models are essential components of AI systems, they do not constitute AI systems on their own. AI models **require the addition of further components** (e.g., a user interface) **to become AI systems**.

AI models are typically integrated into and form part of AI systems.

### Displays significant generality and is capable of competently performing a wide range of distinct tasks

These models are typically trained on large amounts of data, through various methods (e.g., self-supervised, unsupervised or reinforcement learning), and may be placed on the market in various ways (e.g., libraries, Application Programming Interface, etc.). This includes large generative AI models, given that they allow for **flexible generation of content** and **can accommodate a wide range of distinctive tasks**.

### Notes

- The EU AI Act provides specific rules for General-purpose AI models, which will also apply when these models are integrated or form part of an AI system;
- AI models used before their placing on the market for the sole purpose of research, development and prototyping activities are not covered by this definition.



# Steptoe | EU AI Act Decoded



## Exclusions - The EU AI Act will not apply to:

**AI systems or models**, including their output, specifically developed and put into service for the **sole purpose of scientific research and development**.

**Research, testing or development activity on AI systems or models prior to their putting into service or placing on the market**, except if tested in real world conditions.

**AI systems released under free and open-source licenses**, unless they are placed on the market or put into service as high-risk AI systems, or as AI systems that are prohibited or subject to transparency obligations.

**AI systems** placed on the market, put into service, used in the EU or whose output is used in the EU **exclusively for military, defence or national security purposes**.

**Non-EU Public authorities and international organizations** when (i) they use **AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation** with the EU or EU Member States; and (ii) provided that they offer **adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals**.

## Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



<https://www.linkedin.com/showcase/ai-data-digital/>



## Contact us



### Anne-Gabrielle Haie

Partner in Steptoe's AI, Data & Digital practice

## Who will the EU AI Act apply to?

### ALL ACTORS ACROSS THE AI VALUE CHAIN

#### Provider

Natural/legal person, public authority, agency or other body that **develops an AI system or a General-Purpose AI (GPAI) model, or that has it developed and placed on the market/put into service in the EU under its own name or trademark.** This includes Providers:

- located/established in the EU or outside of the EU, and placing on the market/putting into service in the EU an AI system or a GPAI model; and
- located/established outside of the EU, and whose AI systems' output is intended to be used in the EU.

#### Deployer

Natural/legal person, public authority, agency or other body **using an AI system under its authority.** This includes Deployers:

- located/established in the EU; and
- located/established outside of the EU, and whose AI systems' output is intended to be used in the EU.

#### Importer

Natural/legal person, located/established in the EU, that **places on the market an AI system that bears the name or trademark of a natural/legal person established outside the EU.**

#### Distributor

Natural/legal person in the supply chain, other than the Provider/the Importer, that **makes an AI system available on the EU market.**

#### Product Manufacturer

Natural/legal person that **places on the market/puts into service an AI system in the EU together with its product and under its own name or trademark.**

#### Authorized representative

Natural/legal person located/established in the EU, who **represents a provider of an AI system or a GPAI model established outside of the EU.**

#### Notes

- The applicability of the EU AI Act is not solely determined by an organization's location or establishment, but also by the use of an AI system's output within the EU. It may thus **apply to organizations based outside of the EU.**
- The **whole AI value chain** is covered and subject to specific obligations.
- The assessment of the **qualification** (i.e., Provider, Deployer, etc.) must be performed **for each system/GPAI model.** The same organization can have **different qualifications depending on the AI system/GPAI model concerned.** Such assessment must be documented.





## RISK OF REQUALIFICATION

**Distributor/Importer/Deployer/other third-party will be considered as Provider** if they:

- put their name/trademark on a high-risk AI system already placed on the market/put into service in the EU;
- make a substantial modification to a high-risk AI system, already placed on the market/put into service in the EU, in such a way that it remains a high-risk AI system; or
- modify the intended purpose of an AI system, including a GPAI system, not classified as high-risk and already placed on the market/put into service in the EU, which makes it become a high-risk AI system.

➤ In such cases, the initial Provider will no longer be considered as the Provider of this specific AI system. However, the initial Provider must closely cooperate with and make information available to the new provider(s), except if the initial Provider has clearly specified that its AI system must not be changed into a high-risk AI system.

**In the case of high-risk AI systems that are safety components of products covered by legislations listed under Annex I - Section A, the Product Manufacturer will be considered as a Provider of high-risk AI system** if it:

- places on the market the AI system together with the product under its name or trademark; or
- puts into service the AI system under its name or trademark after the product has been placed on the market.

## Notes

- The **qualification may change over time depending on what is done with the AI system**. It is thus important to regularly review the assessment of the qualification.
- Distributor/Importer/Deployer/other third-party/Product Manufacturer requalified as Provider will be **subject to the obligations listed under Article 16 of the EU AI Act**.



## Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



<https://www.linkedin.com/showcase/ai-data-digital/>



## Contact us



**Anne-Gabrielle Haie**

Partner in Steptoe's AI, Data & Digital practice

## Key dates

2024

Establishment  
of the **EU AI  
Office**

February  
21

July  
12

Publication  
of the EU AI  
Act at the  
EU Official  
Journal

August  
1

Entry into  
force of  
the EU AI  
Act

2025

February  
2

Entry into  
application of:

- **General provisions**  
(Chapter I: subject  
matter, scope,  
definitions, obligation  
related to AI literacy)
- Provisions related  
to **Prohibited AI  
practices**  
(Chapter II)

EU Member States must  
have designated their  
**National Competent  
Authorities**

August  
2

Entry into  
application of:

- Obligations  
applicable to  
**General-Purpose AI  
(GPAI) models**  
(Chapter V)
- Provisions related to  
**Governance**  
(Chapter III Section 4 and  
Chapter VII: European AI  
Board, Advisory forum,  
Scientific panel of  
independent experts,  
National Competent  
Authorities)
- Provisions related to  
**penalties for non-  
compliance with the  
EU AI Act** (Chapter XII),  
except for provision  
related to fines for  
Providers of GPAI models  
(Art.101)

2026

August  
2

Entry into application of:

- Obligations applicable to **High-risk AI systems referred in Annex III** (Chapter III Section 1, 2, 3 & 5, and Chapter IX)
- Obligations applicable to **AI systems that are subject to specific transparency obligations** (Chapter IV)
- **Measures in support of innovation**  
(Chapter VI: AI regulatory sandboxes,  
testing in real world conditions,  
Measures for SMEs and Startups)
- Provisions related to **EU Database for High-Risk AI Systems** (Chapter VIII)
- Provisions related to **Remedies**  
(Chapter IX Section 4)
- Provisions related to **Codes of conduct & Guidelines** (Chapter X)
- Provision related to **fines for Providers of GPAI models** (Art.101)

2027

August  
2

Entry into application of:

- Obligations applicable to **High-risk AI systems intended to be used as a safety component of a product/which are themselves products** (i) covered by EU legislations listed under **Annex I**; and (ii) subject to a third-party conformity assessment procedure (Chapter III Section 1, 2, 3 & 5, and Chapter IX)

# Step toe | EU AI Act Decoded



## EXCEPTIONS APPLICABLE TO AI SYSTEMS ALREADY PLACED ON THE MARKET / PUT INTO SERVICE & GPAI MODELS ALREADY PLACED ON THE MARKET

Operators of AI systems that are components of large-scale IT systems in the area of Freedom, Security and Justice established by legal acts listed in Annex X and that have been placed on the market / put into service before August 2, 2027 must comply with the EU AI Act **by 31 December 2030**.

Operators of High-risk AI systems placed on the market/put into service before August 2, 2026, must comply with the EU AI Act only if, as from that August 2, 2026, those systems are subject to significant changes in their designs.

Providers and Deployers of High-risk AI systems intended to be used by public authorities must comply with the EU AI Act by **August 2, 2030**.

Providers of GPAI models placed on the market before August 2, 2025 must comply with the EU AI Act by **August 2, 2027**.

## Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



 <https://www.linkedin.com/showcase/ai-data-digital/>

## Contact us



**Anne-Gabrielle Haie**

Partner in Step toe's AI, Data & Digital practice



## Notes

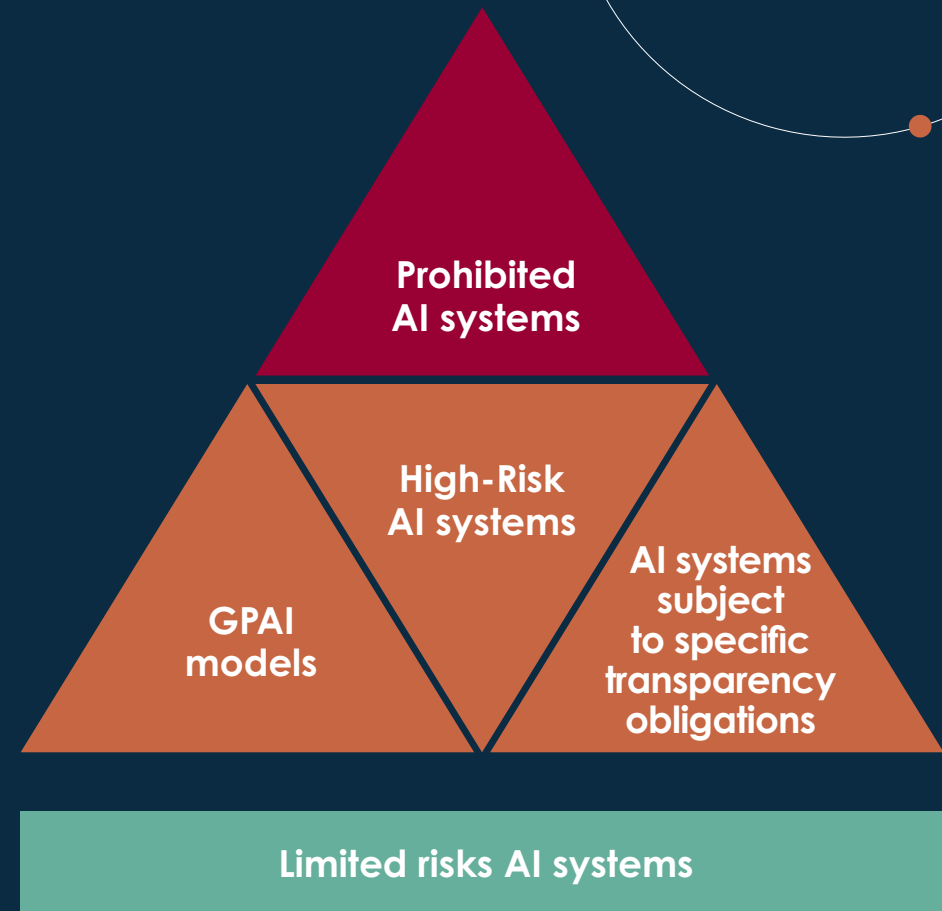
- **Most of the provisions of the EU AI Act** will become **applicable on August 2, 2026**. However, **certain provisions of the EU AI Act will apply either earlier or later than this date**.
- The **timeframe for application of the different provisions of the EU AI Act varies depending on factors such as the classification of an AI system (i.e., as prohibited, high-risk, etc.); the date when an AI system/GPAI model is placed on the market / put into service in the EU; the purpose for which the AI system is used; etc.**
- It is thus **critical to start early with the inventory and the assessment of the classification of the AI system(s) / GPAI model(s) used in your organization in order to identify your compliance deadline(s)**.



## Classification of AI systems and GPAI Models

The EU AI Act classifies AI systems and General-purpose AI (GPAI) models on the basis of the level of risk they pose and the purpose they have. In a nutshell:

- Some AI Systems will be **prohibited** in the EU;
- Some AI Systems will be classified as **high-risk** and will be subject to stringent pre-market and post-market obligations;
- Some AI Systems will be **subject to specific transparency obligations**; and
- Specific rules will apply to **GPAI Models**.



### Notes:

- The main purpose of the EU AI Act is to ensure that safe and trustworthy AI systems are used in the EU. Accordingly, EU legislators have decided to adopt a risk-based approach, with the concept of risk being defined as “the combination of the probability of an occurrence of harm and the severity of that harm”.
- Such a classification is **not mutually exclusive**, e.g. an AI System can be classified as high-risk and be subject to specific transparency obligations at the same time.
- The assessment of the classification of an AI System/GPAI Model must be **performed on a case-by-case basis, documented, reviewed regularly and be kept up-to-date**.
- The EU AI Act does not include any specific obligation for limited risks AI systems; however Providers and Deployers of **limited risks AI systems** will **still be subject to the AI literacy obligation**, which entails taking measures to ensure their staff and other persons dealing with the operation and use of AI systems have the appropriate skills, knowledge and understanding to allow them to make an informed deployment of AI systems, as well as to be aware of the opportunities, risks, and possible harm that AI system can cause.



## Prohibited AI Systems

### AI systems that deploy subliminal techniques beyond a person's consciousness / purposefully manipulative/ deceptive techniques

which materially distort a person's / group's behaviour by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause significant harm

**AI systems for the evaluation / classification of individuals / groups based on their social behaviour/ personal or personality characteristics**, leading to detrimental or unfavourable treatment in unrelated social contexts or unjustified or disproportionate treatment

**AI systems making risk assessments on the risk of a person to commit a criminal offence**, based solely on profiling or on assessment of personality traits and characteristics



Except if used to support the human assessment of the involvement of a person in a criminal activity

**AI systems for biometric categorisation that individually categorise individuals based on their biometric data to deduce / infer sensitive data**



Except labelling / filtering of lawfully acquired biometric datasets based on biometric data / categorizing of biometric data in the area of law enforcement

**AI systems exploiting an individual's / group's vulnerabilities**, which materially distort their behaviour in a manner that causes or is likely to cause significant harm

**AI systems to infer emotions of an individual in the workplace and education institutions**



Except if used for medical or safety reasons

**AI systems that create or expand facial recognition databases through the untargeted scraping of facial images** from the internet / CCTV footage

**AI systems for real-time remote biometric identification in publicly accessible spaces for the purposes of law enforcement**



Except if strictly necessary for limited law enforcement purposes

**AI systems infringing other EU laws**



### Notes:

- The abovementioned AI systems will be **completely banned from the EU from 2 February 2025**, and it will not be possible to place them / put them into service / use them on the EU market.
- It is important to understand the differences amongst the concepts of:
  - **Biometric categorization system** refers to an AI system for the purpose of **assigning individuals to specific categories on the basis of their biometric data**;
  - **Remote biometric identification system** refers to an AI system for the purpose of **identifying individuals**, without their active involvement, typically at a distance **through the comparison of an individual's biometric data with the biometric data contained in a reference database**;
  - **Biometric verification system** refers to the **automated, one-to-one verification, including authentication, of an individual's identity by comparing their biometric data to previously provided biometric data**.
- ➔ Only Biometric categorization systems and Remote biometric identification systems meeting the conditions identified above will be prohibited. Conversely, biometric verification systems do not qualify as "Prohibited AI systems".
- Permitted AI systems for real-time remote biometric identification in publicly accessible spaces for the purposes of law enforcement will be subject to onerous obligations (e.g., prior administrative / judicial authorization; fundamental rights impact assessment; etc.).

## High-risk AI Systems

- AI Systems intended to be used as a safety component of a product/which are themselves products (i) covered by below EU legislations (referenced in Annex I); and (ii) subject to a third-party conformity assessment procedure

### Annex I Section A

Machinery Regulation	Directive on safety of toys	Directive on recreational craft and personal watercraft
Directive on lifts and safety components for lifts	Directive on equipment and protective systems intended for use in potentially explosive atmospheres	Directive on radio equipment
Directive on pressure equipment	Regulation on cableway installations	Regulation on personal protective equipment
Regulation on appliances burning gaseous fuels	Medical devices Regulation	In vitro diagnostic medical devices Regulation

### Annex I Section B

Regulation on common rules in the field of civil aviation security	Regulation on common rules in the field of civil aviation
Regulation on the approval and market surveillance of two- or three-wheel vehicles and quadricycles	Regulation on the approval and market surveillance of agricultural and forestry vehicles
Directive on marine equipment	Directive on the interoperability of the rail system within the EU
Regulation on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles	Regulation on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles



These High-risk AI systems falling under Annex I Section B are **not subject to the requirements for High-risk AI systems laid down under Chapter III Section 2**, of the EU AI Act. The requirements that they will need to comply with will be **integrated into the product legislation's technical specifications and procedures**.

## High-risk AI Systems

- AI Systems used in the below areas (referenced in Annex III)

### Administration of justice and democratic processes

- to be used by judicial authorities / on their behalf to assist in researching and interpreting facts / law application / alternative dispute resolution
- to be used for influencing the outcome of an election / referendum / voting behavior

### Access to and enjoyment of essential private / public services and benefits

- to be used by public authorities / on behalf of public authorities regarding access to essential public assistance benefits and services (e.g., healthcare services)
- to evaluate creditworthiness / establish credit score (except if used to detect financial fraud)
- for risk assessment and pricing in the case of life and health insurance
- to evaluate / classify / dispatch / prioritize emergency calls

### Law enforcement

- to be used by / on behalf of law enforcement authorities for risk assessment of an individual becoming the victim of criminal offences
- polygraphs or similar tools
- to evaluate the reliability of evidence in the criminal investigation / prosecution
- for risk assessment of an individual offending / re-offending or to assess personality traits and characteristics / past criminal behavior
- for profiling of individual in the detection / investigation / prosecution of criminal offences

### Employment, workers' management and access to self-employment

- for recruitment / selection
- to make decisions affecting the work-related relationship

### Migration, asylum and border control management

- to be used by / on behalf of competent public authorities as polygraphs or similar tools
- for risk assessment of an individual intending to enter / who has entered into the EU territory
- for the examination of asylum / visa / residence permit applications and associated complaints
- for the purpose of detecting / recognizing / identifying natural persons (except if used for verification of travel documents)

### Critical infrastructure

- safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity

### Education and vocational training

- to determine access / admission or to assign natural persons to educational and vocational training institutions at all levels
- to evaluate learning outcomes
- for the purpose of assessing the appropriate level of education for an individual
- for monitoring and detecting prohibited behavior of students during tests

### Biometrics

- remote biometric identification systems
- biometric categorization according to sensitive / protected attributes or characteristics
- emotion recognition



## Exception

An AI system used in one of these areas **will not be considered as high-risk** where it **does not pose a significant risk of harm to the health / safety / fundamental rights** and where it **meets either of these conditions**:

- It is intended to perform a **narrow procedural task**;
- It is intended to improve **the result of a previously completed human activity**;
- It is intended to **detect decision-making patterns or deviations** from prior decision-making patterns and which are not meant to replace or influence the previously completed human assessment, without proper human review; or
- It is intended to **perform a preparatory task** to an assessment.

## Notes

- Safety component** must be understood as a component of a product / AI system which fulfils a safety function for that product / AI system, or the failure / malfunctioning of which endangers the health and safety of persons / property.
- For **High-risk AI systems intended to be used as a safety component** of a product/which are themselves products covered by legislations referred to in Annex I, it will be important to **first assess the applicability of the relevant legislations**.
- For AI systems covered by Annex I Section B, it will be important to monitor the adoption of the product legislation's technical specifications and procedures.
- The **list of High-risk AI systems referred to in Annex III** may be **updated from time to time** by the European Commission.
- A provider who considers that an **AI system referred to in Annex III is not high-risk must document its assessment**. It will however remain subject to the obligation to register its AI systems in the EU database for high-risk AI systems.
- AI systems referred to in Annex III** that perform **profiling of individuals** will be **always classified as high-risk**.



## AI systems subject to specific transparency obligations

### AI systems intended to interact directly with natural persons



Except AI systems authorised by law to detect / prevent / investigate / prosecute criminal offences

### AI systems generating synthetic audio, image, video or text content (incl. GPAI)



Except AI systems performing an assistive function for standard editing; that do not substantially alter the input data provided; authorised by law to detect / prevent, investigate / prosecute criminal offences

### Emotion recognition systems / Biometric categorisation systems



Except AI systems permitted by law to detect / prevent / investigate criminal offences

### AI systems generating or manipulating image, audio or video content constituting a deep fake / that generate or manipulate text published for information purpose on matters of public interest



Except AI systems authorised by law to detect / prevent / investigate / prosecute criminal offences, or where the AI-generated content has undergone a process of human review / editorial control under the editorial responsibility of an individual

#### Notes:

- The obligations provided for “AI systems subject to specific transparency obligations” may apply in addition to the obligations foreseen for High-risk AI systems.
- Further clarification from regulators will be necessary regarding the notion of “AI Systems intended to interact directly with natural persons” as it can be understood very broadly and can potentially capture a wide range of AI Systems.



## GPAI Models

- **GPAI Model:** AI model 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**.
- A GPAI model will be classified as a **GPAI model with systemic risk** and be subject to **additional obligations** if it meets either of the following conditions:
  - **it has high impact capabilities** → Presumption of high impact capabilities when the cumulative amount of computation used for its training measured in floating point operations is greater than  $10^{25}$ ; or
  - **it has capabilities / impact equivalent to a GPAI model with high impact capabilities** (based on the number of parameters; quality/size of the data set; amount of computation used for training the model; etc.).



A provider of a GPAI model that meets one of the conditions to be classified as GPAI model with systemic risk may argue that the GPAI model does not present, due its specific characteristics, systemic risks and should therefore not be classified as such.

## Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



<https://www.linkedin.com/showcase/ai-data-digital/>



## Contact us



**Anne-Gabrielle Haie**

Partner in Steptoe's AI, Data & Digital practice



### Notes:

- AI models that are used for research, development or prototyping activities before they are placed on the market are excluded from the definition of GPAI model, and thus they are not subject to the obligations applicable to GPAI models.
- Providers of GPAI model meeting one of the conditions to be classified as GPAI model with systemic risk must notify the European Commission without undue delay and in any event within 2 weeks after the condition is met / it becomes known that the condition will be met.
- The European Commission may decide, at its own volition or following a qualified alert from the scientific panel, to classify a GPAI model as a GPAI model with systemic risk.
- The list of GPAI models with systemic risk will be published.
- Thresholds, tools and benchmarks used to assess whether a GPAI model has high-impact capabilities or capabilities/impact equivalent to GPAI models with high impact capabilities can be amended by the European Commission in light of evolving technological developments.



## Obligations for Providers of High-risk AI systems

For a refresher on the notions of “Provider” and “High-risk AI systems”, please consult our previous EU AI Act Decoded issues on “[Who will the EU AI Act apply to?](#)” and “[Classification of AI systems and GPAI Models](#)”

### Implement risk management system

(Art. 9)

This must comprise:

- identification and analysis of the **known and reasonably foreseeable risks** that can be posed by the AI system to **health, safety or fundamental rights** when used in accordance with its intended purpose;
- estimation and evaluation of the **risks that may emerge when the AI system is used in accordance with its intended purpose**, and under conditions of **reasonably foreseeable misuse**;
- evaluation of **other risks possibly arising**, based on the analysis of data gathered from the **post-market monitoring system**;
- **after testing**, adoption of appropriate and targeted **risk management measures** designed to address the known and the reasonably foreseeable risks.

→ **Continuous iterative process to be run throughout the entire lifecycle of the AI system**

### Implement data governance and management practices for training, validation and testing data

(Art. 10)

These practices must cover in particular:

- relevant **design choices**;
- **data collection and origin processes** (in the case of personal data, this includes the original purpose of the data collection);
- relevant **data-preparation processing operations** (e.g., annotation, labelling, cleaning, updating, enrichment and aggregation);
- **formulation of assumptions**, in particular with respect to the information that the data are supposed to measure and represent;
- assessment of the **availability, quantity and suitability** of the data sets needed;
- examination of **possible biases** that are likely to affect individuals' health and safety / have a negative impact on fundamental rights / lead to prohibited discrimination, especially where data outputs influence inputs for future operations;
- appropriate **measures to detect, prevent and mitigate possible biases**;
- identification of relevant **data gaps / shortcomings** that prevent compliance with the EU AI Act, and how those gaps and shortcomings can be addressed.

**Training, validation and testing data sets** must meet the following **quality criteria**:

- relevant;
- sufficiently representative;
- free of errors (to the extent possible);
- complete in view of the intended purpose;
- have the appropriate statistical properties;
- take into account the characteristics elements that are particular to the specific geographical, contextual, behavioral or functional setting within which the AI system is intended to be used.

⚠ Where strictly necessary for bias detection and correction, special categories of personal data may be processed subject to certain conditions.

### Draft technical documentation containing, at least, the elements set out in Annex IV of the EU AI Act

(Art. 11)

It must be drawn up **prior to the placing on the market / putting into service of the AI system**, and **kept up-to date**.

⚠ Annex IV may be amended, from time to time, by the European Commission

⚠ SMEs, including start-ups, may provide the technical documentation in a simplified manner (form to be issued by European Commission)

## Design AI system to allow for the automatic recording of events (logs) over its lifetime

(Art. 12)

⚠️ Specific logging capabilities must be met for AI systems used for remote biometrics identification systems covered by Annex III, 1. (a).

## Design AI system to ensure that its operation is sufficiently transparent to enable deployers to interpret its output and use it appropriately

+

### Draft instructions for use

(Art. 13)

The instructions for use must at least contain:

- **identity and contact details of the provider** and, where applicable, of its authorized representative;
- **characteristics, capabilities and limitations of performance of the AI system**, including:
  - its **intended purpose**;
  - the **level of accuracy**, including its metrics, robustness and cybersecurity against which it has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;
  - any **known or foreseeable circumstances**, related to its use in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, **which may lead to risks to the health and safety or fundamental rights**;
  - where applicable, its **technical capabilities and characteristics** to provide relevant information to explain its output;
  - when appropriate, its **performance** regarding specific persons or groups of persons on which the system is intended to be used;
  - when appropriate, **specifications for the input data**, or any other relevant information in terms of the training, validation and testing data sets used, taking into account its intended purpose;
  - where applicable, **information to enable deployers to interpret its output** and use it appropriately;
- the **changes to the AI system and its performance which have been pre-determined** at the moment of the initial conformity assessment, if any;
- the **human oversight measures** implemented (incl. technical measures put in place to facilitate the interpretation of the outputs of the AI system by the deployers);
- the **computational and hardware resources needed**, the **expected lifetime** of the AI system and any necessary **maintenance and care measures** (incl. their frequency) to ensure the proper functioning of the AI system (incl. software updates);
- where relevant, a **description of the mechanisms** included within the AI system that allows deployers to **properly collect, store and interpret the logs**.

## Design AI system to ensure effective human oversight when in use in order to prevent / minimize risks to health / safety / fundamental rights

(Art. 14)

This must be achieved through the implementation of measures built into the AI system by the provider, and/or to be implemented by the deployer that enable individual(s) in charge of human oversight at the deployer to:

- properly understand the **relevant capacities and limitations of the AI system and be able to duly monitor its operation** (incl. in view of detecting and addressing anomalies, dysfunctions and unexpected performance);
- remain aware of the **possible tendency of automatically relying or over-relying on the output produced by the AI system** (automation bias), in particular for AI system used to provide information or recommendations for decisions to be taken by natural persons;
- correctly **interpret the AI system's output** (e.g., considering the interpretation tools and methods available);
- decide, in any particular situation, **not to use the AI system or to otherwise disregard, override or reverse its output**;
- **intervene in the operation of the AI system / interrupt it** through a "stop" button or a similar procedure that allows the system to come to a halt in a safe state.

⚠️ Specific measures required for remote biometrics identification systems covered by Annex III, 1. (a).

## Design and implement technical and organizational measures to ensure that the AI system achieves an appropriate level of accuracy, robustness, and cybersecurity throughout its lifecycle

(Art. 15)

This must be achieved through the implementation of **technical and organizational measures** to:

- ensure that the AI system is as **resilient** as possible **regarding errors, faults or inconsistencies** that may occur within the system or the environment in which it operates, in particular due to their interaction with individuals or other systems (e.g., technical redundancy solutions, such as backup or fail-safe plans);
- eliminate / reduce as far as possible the **risk of possibly biased outputs** influencing input for future operations (feedback loops), and to ensure that any such feedback loops are duly addressed with appropriate mitigation measures for any AI system that continues to learn after being placed on the market / put into service;
- ensure **resiliency against attempts by unauthorized third parties** to alter their use / outputs / performance by exploiting system vulnerabilities (incl. where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks or model flaws).

→ **Levels of accuracy and relevant accuracy metrics of the AI system must be declared in the instructions for use.**

## Implement a Quality Management System

(Art. 17)

The quality management system must include **written policies, procedures and instructions**, covering at least the following aspects:

- **strategy for regulatory compliance** (incl. compliance with conformity assessment procedures and procedures for the management of modifications to AI system);
- techniques, procedures and systematic actions to be used for the **design, design control and design verification** of the AI system;
- techniques, procedures and systematic actions to be used for the **development, quality control and quality assurance** of the AI system;
- **examination, test and validation procedures** to be carried out before, during and after the development of the AI system, and the frequency with which they have to be carried out;
- **technical specifications** (incl. standards) to be applied and, where the relevant harmonized standards are not applied in full or do not cover all of the applicable requirements, the means to be used to ensure that the AI system complies with those requirements;
- systems and procedures for **data management**, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding data that is performed before and for the purpose of the placing on the market / the putting into service of AI system;
- the **risk management system**;
- the setting-up, implementation and maintenance of a **post-market monitoring system**;
- procedures related to the **reporting of a serious incident**;
- handling of **communication** with competent authorities, other operators, customers or other interested parties;
- systems and procedures for **record-keeping of documentation and information**;
- **resource management** (incl. security-of-supply related measures);
- **accountability framework** setting out the responsibilities of the management and other staff with regard to all the aspects covered by the quality management system.

## Keep documentation, at the disposal of national competent authorities, for 10 years after the placing on the market / putting into service of the AI system

(Art. 18)

This includes:

- the **technical documentation**;
- the documentation concerning the **quality management system**;
- the **documentation concerning the changes** approved by notified bodies, where applicable;
- the **decisions and other documents issued by the notified bodies**, where applicable; and
- the **EU declaration of conformity**.

**Keep automatically generated logs - to the extent that such logs are under control - for a period of at least 6 months**

(Art. 19)

This obligation is subject to applicable laws, which may provide for a different retention period.

**Inform relevant stakeholders and implement corrective actions in case of non-conformity / risk**

(Art. 20)

- Where there is reason to consider that the AI system placed on the market / put into service is not in conformity with the EU AI Act, the Provider must:
  - take the necessary corrective actions to bring that system into conformity / withdraw / disable / recall it;
  - inform the distributors, deployers, authorized representative and importers.
- Where the AI system presents a risk (= could affect adversely individuals' health / safety / fundamental right to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use), the Provider must:
  - investigate the causes (where applicable, in collaboration with the reporting deployer);
  - inform the competent market surveillance authority(ies); and where applicable, the competent notified body of the nature of the non-compliance and of any relevant corrective action taken.

**Undergo a Conformity Assessment prior to placing on the market / putting into service the AI system**

(Art. 43, 44 & 46)

**Different conformity assessment procedures apply depending the category of high-risk AI systems.**

- ➔ Undergoing a conformity assessment procedure may not be necessary in case of compliance with harmonized standards or common specifications.
- ⚠ The European Commission may amend, from time to time, the conformity assessment requirements and procedures.
- ⚠ Under specific circumstances, market surveillance authorities may grant derogation from conformity assessment procedure.

**Draw up EU declaration of conformity & affix the CE marking on the AI system**

(Art. 47 & 48)

- The Provider must draw up an EU declaration of conformity containing the information set out in Annex V for each AI system. The EU declaration of conformity must be kept at the disposal of the competent authorities for 10 years after the high-risk AI system has been placed on the market / put into service.
- ⚠ The European Commission may amend, from time to time, the content of the EU declaration of conformity.
- The Provider must affix the CE marking on the AI system physically or digitally.

**Register the AI system in the EU database**

(Art. 49)

- **AI systems listed in Annex III** (except those used for critical infrastructures listed under Annex III 2, which must be registered at national level) must **be registered in the EU database** for high-risk AI systems before their placing on the market / putting into service.
- ⚠ AI systems for which the Provider has concluded that it is not high-risk according to Article 6 (3) of the EU AI Act must also be registered in this EU database before their placing on the market / putting into service.

## Implement a Post-Market Monitoring System

(Art. 72)

- The post-market monitoring system must be based on a **post-market monitoring plan**, which must be part of the technical documentation.
- ⚠ The European Commission will adopt a template for the post-market monitoring by 2 February 2026.
- The post-market monitoring system must actively and systematically collect, document and analyze relevant data provided by deployers or collected through other sources on the performance of the AI system throughout its lifetime, and which allow the Provider to evaluate the continuous compliance of the AI system with the EU AI Act. Where relevant, it must include an analysis of the interaction with other AI systems.

## Report serious incidents to national market surveillance authority(ies) and investigate them

(Art. 73)

- **Serious incidents** (= an incident / malfunctioning of an AI system that directly / indirectly leads to the death of an individual or serious harm to his/her health; a serious and irreversible disruption of the management or operation of critical infrastructure; the infringement of obligations under EU law intended to protect fundamental rights; or serious harm to property or the environment) **must be reported to the national market surveillance authority(ies)** where that incident occurred:
  - **immediately** after the provider has established a causal link between the AI system and the serious incident or the reasonable likelihood of such a link, and, in any event, **not later than 15 days** after the provider becomes aware of the serious incident;
  - **immediately, and not later than 2 days** after the provider becomes aware of that incident in the event of a **widespread infringement** / in the case of a **serious and irreversible disruption of the management or operation of critical infrastructure**;
  - **immediately** after the provider has established / as soon as it suspects, a **causal relationship** between the high-risk AI system and the serious incident, but **not later than 10 days** after the date on which the provider becomes aware of the serious incident in the event of the **death of an individual**.
- Following the reporting, the provider must, without delay, perform the necessary investigations in relation to the serious incident, which include a risk assessment of the incident and corrective action.
- ⚠ For AI systems under Annex III placed on the market / put into service by providers subject to **EU laws** laying down equivalent reporting obligations, and AI systems under Annex I subject to Medical Devices Regulation and In Vitro Diagnostic Medical Devices Regulation, the reporting obligation is limited to serious incident leading to the infringement of obligations under EU law intended to protect fundamental rights.

## Indicate name, registered trade name / trade mark, address on the AI system

(Art. 16)

If it is not possible to indicate such information on the AI system, this must be included on its packaging or accompanying documentation.

## For Providers established outside of the EU, appoint an authorized representative established in the EU

(Art. 22)

The authorized representative must be appointed by written mandate.

## Design AI system in compliance with EU law accessibility requirements

(Art. 16)

This includes compliance with requirements provided by:

- Directive (EU) 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies; and
- Directive (EU) 2019/882 on the accessibility requirements for products and services.

## Implement AI literacy measures

(Art. 4)

This includes measures to ensure the Provider's staff and other persons dealing with the operation and use of the AI system have the **appropriate skills, knowledge and understanding** to allow them to make an informed deployment of the AI system, as well as to be aware of the opportunities, risks, and possible harm that AI system can cause.



## Deadline to comply with these obligations:

August  
2  
2026

For Providers of High-risk AI systems referred in **Annex III**

August  
2  
2027

For Providers High-risk AI systems intended to be used as a safety component of a product/which are themselves products (i) covered by EU legislations listed under **Annex I**; and (ii) subject to a third-party conformity assessment procedure

### Notes:


- The EU AI Act provides for **stringent post-market and pre-market obligations** for Providers of high-risk AI systems that span **across their lifecycle**.
- The **intended purpose of the AI system** as well as the **generally acknowledged state of the art of AI and AI-related technologies must be taken into account** when determining the steps and measures required to comply with the above obligations.
- Compliance with all of the above obligations must be **documented**.
- **Some compliance measures must be specific to each high-risk AI system** (e.g., technical documentation), **while others could be common to all high-risk AI systems** (e.g. AI literacy measures).
- For providers that are subject to similar requirements under relevant provisions of other EU laws (incl. financial institutions), compliance with the above obligations may be **integrated into compliance documentation drawn up under this other EU law**.
- Providers bear an **obligation of cooperation** with competent authorities, which notably entails the obligation to provide all the information and documentation necessary to demonstrate compliance.
- Providers must **closely monitor regulatory developments** including any templates to be issued by the European Commission / EU AI Office / national competent authorities.



## Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



 [linkedin.com/showcase/ai-data-digital](https://www.linkedin.com/showcase/ai-data-digital)

## Contact us



**Anne-Gabrielle Haie**

Partner in Steptoe's AI, Data & Digital practice



## Obligations for Deployers of High-risk AI systems

For a refresher on the notions of “Deployer” and “High-risk AI systems”, please consult our previous EU AI Act Decoded issues on “[Who will the EU AI Act apply to?](#)” and “[Classification of AI systems and GPAI Models](#)”

**Implement technical and organizational measures to ensure that the AI system is used in accordance with the instructions for use**

(Art. 26)

This includes, notably, technical and organizational measures to **monitor the operation of the AI system** on the basis of the instructions for use.

**Assign responsibility to oversee the AI system to competent individual(s) and provide necessary support**

(Art. 26)

The responsibility to oversee the AI system must be assigned to **individual(s) who have the necessary competence, training and authority**, as well as the necessary support.

**Implement practices to ensure data quality**

(Art. 26)

To the extent that the Deployer exercises control over the input data, it must implement **practices to ensure that input data is relevant and sufficiently representative** in view of the intended purpose of the AI system.

**Monitor the operation of the AI system**

(Art. 26)

- The Deployer must monitor the operation of the AI system on the basis of the instructions for use.
- Where relevant, the Deployer must inform the Provider in accordance with the Provider’s post-market monitoring plan.

**Inform relevant stakeholders in case of risk and suspend the use of the AI system**

(Art. 26)

Where the Deployer has reason to consider that **the use of the AI system in accordance with the instructions may result in a risk** (= could affect adversely individuals’ health / safety / fundamental rights to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use), it must **suspend the use of that AI system, and inform** without undue delay:

- the Provider / Distributor; and
- the relevant market surveillance authority(ies) and shall suspend the use of that system.

## Report serious incidents to relevant stakeholders

(Art. 26 & 73)

- Where the Deployer has identified a **serious incident** (= an incident / malfunctioning of an AI system that directly / indirectly leads to the death of an individual or serious harm to his/her health; a serious and irreversible disruption of the management or operation of critical infrastructure; the infringement of obligations under EU law intended to protect fundamental rights; or serious harm to property or the environment), the Deployer must immediately **inform** and in the below order:
  - the Provider;
  - the Importer / Distributor; and
  - the competent market surveillance authority(ies).

⚠ If the Deployer is not able to reach the Provider, the Deployer must report the serious incident to the national market surveillance authority(ies) where that incident occurred:

- not later than **15 days** after the Deployer becomes aware of the serious incident;
- immediately, and **not later than 2 days** after the Deployer becomes aware of that incident in the event of a **widespread infringement / in the case of a serious and irreversible disruption of the management or operation of critical infrastructure**;
- immediately after the Deployer has established / as soon as it suspects, a causal relationship between the high-risk AI system and the serious incident, but **not later than 10 days** after the date on which the Deployer becomes aware of the serious incident in the event of the **death of an individual**.

## Keep automatically generated logs - to the extent that such logs are under control - for a period of at least 6 months

(Art. 26)

This obligation is subject to applicable laws, which may provide for a different retention period.

## Inform workers' representatives and affected workers of the use of the AI system prior to its deployment

(Art. 26)

The information that workers will be subject to the use of the AI system must be provided in accordance with the rules and procedures laid down in EU and national law and practice on information of workers and their representatives.

## Where applicable, register in the EU database

(Art. 26)

⚠ This obligation **applies solely to Deployers that are public authorities, EU institutions / bodies / offices / agencies, or persons acting on their behalf**. Other Deployers can register on a voluntarily basis.


- Before putting into service or using **AI systems listed in Annex III** (except those used for critical infrastructures listed under Annex III 2. which will be registered at national level), public authorities, EU institutions / bodies / offices / agencies, or persons acting on their behalf must register themselves, select the system and register its use in the EU database for high-risk AI systems.

⚠ If the AI system envisaged to be used has not been priorly registered in the EU database by the Provider / the Authorized Representative, the concerned Deployers **must not use this AI system** and must inform the Provider / the Distributor.

## Inform individuals that they will be subject to the use of the AI system

(Art. 26)

- This obligation applies when the AI system is used to make decisions or assist in making decisions related to individuals.
- This information should include the **intended purpose and the type of decisions it makes**. The Deployer should also inform the individuals about their **right to an explanation** provided under the EU AI Act.

 Specific obligations apply for AI systems used for law enforcement purposes.

## Conduct a Fundamental Rights Impact Assessment (FRIA) and notify the competent market surveillance authority

(Art. 27)

- Prior to the deployment of the AI system, a FRIA must be conducted by:
  - **Deployers that are bodies governed by public law / private entities providing public services when using an AI system referred to in Annex III** (with the exception of used for critical infrastructures listed under Annex III 2.); and
  - **Deployers when using an AI system to evaluate the creditworthiness of individuals or establish their credit score** (Annex III 5. b), and when using an AI system for **risk assessment and pricing in relation to individuals in the case of life and health insurance** (Annex III 5. c).
- The FRIA must cover the following aspects:
  - description of the Deployer's processes in which the AI system will be used in line with its intended purpose;
  - description of the period of time within which, and the frequency with which, the AI system is intended to be used;
  - categories of individuals / groups likely to be affected by its use in the specific context;
  - the specific risks of harm likely to have an impact on these categories of individuals / group, considering the information provided in the instructions for use;
  - description of the human oversight measures implemented;
  - the measures to be taken in the case of the materialization of those risks, including the arrangements for internal governance and complaint mechanisms.
- ➔ The obligation to conduct a FRIA applies to the **first use of the AI system**. The Deployer may thus rely on previously conducted FRIA(s) / existing impact assessments carried out by Provider. If, during the use of the AI system, any of elements has changed / is no longer up to date, the Deployer must update the information.
- Where relevant, the FRIA may complement the information gathered in the context of the conduct of data protection impact assessment under the General Data Protection Regulation (GDPR).
- The **results of the FRIA must be notified to the competent market surveillance authority**. Such notification must include the filled-in FRIA questionnaire.

 The AI Office will develop a template questionnaire to conduct FRIA.

## Implement AI literacy measures

(Art. 4)

This includes measures to ensure the Provider's staff and other persons dealing with the operation and use of the AI system have the **appropriate skills, knowledge and understanding** to allow them to make an informed deployment of the AI system, as well as to be aware of the opportunities, risks, and possible harm that AI system can cause.



## Deadline to comply with these obligations:

August  
2  
2026

For Deployers of High-risk AI systems referred in Annex III

August  
2  
2027

For Deployers High-risk AI systems intended to be used as a safety component of a product/which are themselves products (i) covered by EU legislations listed under Annex I; and (ii) subject to a third-party conformity assessment procedure

### Notes:


- The **intended purpose of the AI system** as well as the **generally acknowledged state of the art of AI and AI-related technologies must be taken into account** when determining the steps and measures required to comply with the above obligations.
- Compliance with all of the above obligations must be **documented**.
- For Deployers that are subject to similar requirements under relevant provisions of other EU laws (incl. financial institutions), compliance with the above obligations may be **integrated into compliance documentation drawn up under these other EU laws**.
- **Specific obligations** apply to Deployers of AI systems used for **post-remote biometric identification**.
- Deployers bear an **obligation of cooperation** with competent authorities, which notably entails the obligation to provide all the information and documentation necessary to demonstrate compliance.
- Deployers must **closely monitor regulatory developments** including any templates to be issued by the European Commission / EU AI Office / national competent authorities.



## Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



 [linkedin.com/showcase/ai-data-digital](https://www.linkedin.com/showcase/ai-data-digital)

## Contact us



**Anne-Gabrielle Haie**  
Partner in Step toe's AI,  
Data & Digital practice



## Obligations for Importers / Distributors / Authorized Representatives of High-risk AI systems

For a refresher on the notions of “Importer”, “Distributor”, “Authorized Representative” and “High-risk AI systems”, please consult our previous EU AI Act Decoded issues on [“Who will the EU AI Act apply to?”](#) and [“Classification of AI Systems and GPAI Models”](#)

### Importers

**Verify Provider's compliance with the EU AI Act prior to placing the AI system on the EU market**

(Art. 23)

- The Importer must verify that the Provider has:
  - undergone the relevant **conformity assessment procedure**;
  - drawn up the **technical documentation** in accordance with the EU AI Act;
  - affixed the required **CE marking** on the AI system and has accompanied the AI system with the **EU declaration of conformity** and **instructions for use**;
  - where relevant, designated an **Authorized Representative**.

⚠ Where the Importer has sufficient reason to consider that the AI system is not in conformity with the EU AI Act / is falsified / is accompanied by falsified documentation, it must not place the AI system on the EU market until it has been brought into conformity.

**Inform relevant stakeholders in case of risk**

(Art. 23)

Where the **AI system presents a risk** (= could affect adversely individuals' health / safety / fundamental rights to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use), the Importer must **inform**:

- the Provider;
- where relevant, the Authorized Representative;
- the relevant market surveillance authority(ies).

**Indicate Importer's name, registered trade name / trade mark, address on the AI system**

(Art. 23)

These must also be indicated on the AI system's packaging / its accompanying documentation, where applicable.

**Ensure the AI system's compliance with the EU AI Act while being under the Importer's responsibility**

(Art. 23)

While the AI system is under its responsibility, the Importer must ensure that the storage / transport conditions of the AI system do not jeopardize its compliance with the EU AI Act.

**Keep relevant documentation for 10 years after the placing on the EU market / putting into service of the AI system**

(Art. 23)

The Importer must keep a copy of:

- where applicable, the certificate issued by the notified body;
- the instructions for use; and
- the EU declaration of conformity.

## Distributors

**Verify Provider's and Importer's compliance with the EU AI Act prior to making the AI system available on the EU market**

(Art. 24)

- The Distributor must verify that:
  - the AI system bears the **required CE marking**, and is accompanied by **a copy of the EU declaration of conformity** and **instructions for use**;
  - the Provider and the Importer have complied with their respective obligations related to (i) the indication of their name, registered trade name / trade mark, and address; and (ii) the implementation of a quality management system.

⚠ Where the Distributor has sufficient reason to consider that the AI system is not in conformity with the EU AI Act, it must not make the AI system available on the EU market until it has been brought into conformity.

**Ensure the AI system's compliance with the EU AI Act while being under the Distributor's responsibility**

(Art. 24)

While the AI system is under its responsibility, the Distributor must ensure that the storage / transport conditions of the AI system do not jeopardize its compliance with the EU AI Act.

**Inform relevant stakeholders and implement corrective actions in case of non-conformity / risk**

(Art. 24)

- Where it has reason to consider that the AI system made available on the EU market is not in conformity with the EU AI Act, the Distributor must:
  - take the necessary **corrective actions** to bring the AI system into conformity / withdraw / recall it; or
  - ensure that the Provider / Importer / any other relevant operator take these corrective actions.
- Where the AI system presents a risk (= could affect adversely individuals' health / safety / fundamental rights to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use), the Distributor must immediately **inform** and give details about the non-compliance and any corrective actions taken to:
  - the Provider / Importer; and
  - the competent authority(ies).

## Authorized Representatives

**Ensure that the appointment as Authorized Representative is made through a written mandate from the Provider**

(Art. 22)

- The written mandate must enable the Authorized Representative to perform all of the tasks assigned to it by the EU AI Act (detailed below).
- The written mandate must empower the Authorized Representative to be addressed, in addition to / instead of the Provider, by competent authorities on all issues related to compliance with the EU AI Act, and to provide them with all required information and documentation (incl. logs when relevant).

**Provide a copy of the written mandate to competent market surveillance authority(ies) upon request**

(Art. 22)

This must be provided in one of the EU official languages as indicated by the competent authority(ies).

**Verify Provider's compliance with the EU AI Act**

(Art. 22)

The Authorized Representative must verify that the Provider has:

- drawn up the EU declaration of conformity and the technical documentation;
- undergone the appropriate conformity assessment procedure.

**Keep relevant documentation for 10 years after the placing on the EU market / putting into service of the AI system**

(Art. 22)

The Authorized Representative must keep at the disposal of competent authorities / bodies:

- the Provider's contact details;
- a copy of the EU declaration of conformity;
- the technical documentation; and
- where applicable, the certificate issued by the notified body.

**Register in the EU Database**

(Art. 22 & 49)

- Before placing on the market / putting into service an AI system listed in Annex III (except those used for critical infrastructures listed under Annex III 2. which must be registered at national level), the Provider/ Authorized Representative must register itself and the AI system in the EU database for High-risk AI systems.
  - Before its placing on the market / putting into service, the Provider / Authorized Representative must also register itself and register the AI system in the EU Database when the Provider has concluded that the AI system is not High-risk according to Article 6 (3) of the EU AI Act.
- ⚠ If the Provider is doing the registration itself, the Authorized Representative must ensure that the Provider is providing the Authorized Representative's correct contact details.

## Authorized Representatives

### Terminate mandate if Provider is infringing the EU AI Act

(Art. 22)

- ⚠ The Authorized Representative must terminate the mandate if it has reason to consider that the Provider is acting contrary to its obligations pursuant to the EU AI Act.
- ⚠ In such a case, the Authorized Representative must immediately inform the relevant market surveillance authority, and, where applicable, the relevant notified body, about the termination of the mandate and the reasons therefor.



### Deadline to comply with these obligations:

August  
2  
2026

For High-risk  
AI systems referred  
in Annex III

August  
2  
2027

For High-risk AI systems intended to be used as  
a safety component of a product/which are  
themselves products (i) covered by EU  
legislations listed under Annex I; and  
(ii) subject to a third-party conformity  
assessment procedure

#### Notes:


- Compliance with all of the above obligations must be **documented**.
  - In certain situations, an **operator could act in more than one role at the same time** and must therefore fulfil cumulatively all the relevant obligations associated with those roles. For example, an organization could cumulatively act as Distributor and Importer.
  - Importers / Distributors / Authorized Representatives bear an **obligation of cooperation** with competent authorities, which notably entails the obligation to provide all the information and documentation necessary to demonstrate compliance.
  - Importers / Distributors / Authorized Representatives must **closely monitor regulatory developments** including any templates to be issued by the European Commission / EU AI Office / national competent authorities.
- ⚠ Depending on what they do with the AI system, the Importer / Distributor may be requalified as Provider and be subject to the obligations listed under Article 16 of the EU AI Act. Please see EU AI Act Decoded issue on "Who will the EU AI Act apply to?" for more information.



## Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



 [linkedin.com/showcase/ai-data-digital](https://www.linkedin.com/showcase/ai-data-digital)

## Contact us



**Anne-Gabrielle Haie**

Partner in Step toe's AI,  
Data & Digital practice



## Obligations for Providers of General-Purpose AI models

For a refresher on the notions of “Provider” and “General-Purpose AI model” (GPAI model), please consult our previous EU AI Act Decoded issues on “[Who will the EU AI Act apply to?](#)” and “[Classification of AI Systems and GPAI Models](#)”

**Draft technical documentation of the GPAI model (incl. its training, testing process, and the results of its evaluation) containing, at least, the elements set out in Annex XI**

(Art. 53)

- It must be kept up-to-date along the lifecycle of the GPAI model.

⚠ This obligation does not apply to Providers of **GPAI models that are released under a free and open-source license** which allows for the access, usage, modification, and distribution of the model, and whose parameters (incl. the weights; information on the model architecture; information on model usage) are made publicly available, unless the GPAI models present systemic risks.

⚠ Annex XI may be amended or further completed, from time to time, by the European Commission.

**Draft and make available information and documentation to downstream Providers that integrate the GPAI model into their AI system**

(Art. 53)

- This technical documentation must contain:
  - information enabling downstream Providers to have a good understanding of the capabilities and limitations of the GPAI model and to comply with their own obligations pursuant to the EU AI Act; and
  - at least, the elements set out in Annex XII.

⚠ This obligation does not apply to Providers of **GPAI models that are released under a free and open-source license** which allows for the access, usage, modification, and distribution of the model, and whose parameters (incl. the weights; information on the model architecture; information on model usage) are made publicly available, unless the GPAI models present systemic risks.

⚠ Annex XII may be amended, from time to time, by the European Commission.

**Implement a copyrights and related rights policy**

(Art. 53)

- This policy must outline the steps taken to comply with EU laws on copyright and related rights, in particular with the reservation of rights pursuant to Article 4 (3) of Directive (EU) 2019/790 (“exception or limitation for text and data mining”).

⚠ This obligation applies irrespective of the jurisdiction in which the copyright-relevant acts underpinning the training of a GPAI model take place, as long as that GPAI model is placed on the EU market.

**Draft and make publicly available a detailed summary of the content used for training of the GPAI model**

(Art. 53)

- This summary must be generally comprehensive in its scope instead of technically detailed to facilitate parties with legitimate interests (including copyright holders) to exercise and enforce their rights under EU laws (e.g., by listing the main data collections or sets that went into training the model, such as large private or public databases or data archives, and by providing a narrative explanation about other data sources used).

⚠ The template to be used will be issued by the European Commission.

**For Providers established outside of the EU, appoint an Authorized Representative established in the EU**

(Art. 54)

- The Authorized Representative must be appointed prior to the placing of the GPAI model on the EU market and by written mandate.

⚠ This obligation does not apply to Providers of **GPAI models that are released under a free and open-source license** which allows for the access, usage, modification, and distribution of the model, and whose parameters (incl. the weights; information on the model architecture; information on model usage) are made publicly available, unless the GPAI models present systemic risks.

## Additional obligations for Providers of GPAI models with systemic risk

For a refresher on the notions of “GPAI model with systemic risk”, please consult our previous EU AI Act Decoded issue on “[Classification of AI systems and GPAI Models](#)”.

**Within two weeks, notify the European Commission when the GPAI model meets or will meet a criterion to be qualified as a GPAI model with systemic risk**

(Art. 52)

- A GPAI model will be classified as a GPAI model with systemic risk if it meets either of the following **criteria**:
  - it has **high impact capabilities** => Presumption of high impact capabilities when the cumulative amount of computation used for its training measured in floating point operations is greater than  $10^{25}$ ; or
  - it has **capabilities / impact equivalent to a GPAI model with high impact capabilities** with regards to the criteria set out in Annex XIII.
- ⚠ The European Commission may, from time to time, update these thresholds, or supplement benchmarks and indicators.
- The notification to the European Commission must:
  - be done without delay and in any event **within two weeks** after either criterion is met or it becomes known that it will be met;
  - include the information necessary to demonstrate that the relevant criterion has been met.
- The Provider of a GPAI model that meets the criterion related to high impact capabilities may present, with its notification, sufficiently substantiated arguments to demonstrate that although it meets this criterion, the GPAI model does not present, due to its specific characteristics, systemic risks and should therefore not be classified as such.
- ⚠ The Commission can designate a GPAI model as a GPAI model with systemic risk even if it has not received a notification.
- ⚠ The list of GPAI models considered as GPAI models with systemic risks will be published by the European Commission.

**Perform GPAI model evaluations in order to identify and mitigate systemic risks**

(Art. 55)

- These model evaluations must be performed in accordance with standardized protocols and tools reflecting the state of the art.
- It must notably comprise conducting and documenting adversarial testing of the GPAI model in order to identify and mitigate systemic risks.
- It must notably be performed prior to its first placing on the market.
- It can be achieved through internal or independent external testing

**Continuously assess possible systemic risks at EU level and implement mitigation measures**

(Art. 55)

- The assessment of the possible systemic risks (incl. their sources) and the definition of the mitigation measures must cover the GPAI model's entire lifecycle.
- This may be achieved by implementing risk-management policies (e.g., accountability and governance processes), post-market monitoring, appropriate measures along the entire model's lifecycle, and cooperating with relevant actors along the AI value chain.

**Keep track, document, and report serious incidents to competent authorities**

(Art. 55)

- Serious incident (= an incident / malfunctioning of a GPAI model that directly / indirectly leads to the death of an individual or serious harm to his/her health; a serious and irreversible disruption of the management or operation of critical infrastructure; the infringement of obligations under EU law intended to protect fundamental rights; or serious harm to property or the environment) must be kept track of, documented, and reported, without undue delay, to the AI Office and, as appropriate, to national competent authorities.
- The report to the AI Office and other competent authorities must include relevant information about the serious incidents and the corrective measures to address them.

## Additional obligations for Providers of GPAI models with systemic risk

### Implement cybersecurity measures to protect the model and its physical infrastructure

(Art. 55)

- These measures should notably address potential accidental model leakage, unauthorized releases, circumvention of safety measures, and defence against cyberattacks, unauthorized access, or model theft.
- These measures may include operational security measures for information security, specific cybersecurity policies, adequate technical and established solutions, and cyber and physical access controls.



### Deadline to comply with these obligations:

August  
2  
2025

Entry into  
application of  
these obligations

August  
2  
2026

Entry into application of enforcement  
measures

#### Notes:


- The abovementioned obligations should apply **once the GPAI model is placed on the market**.
- When the Provider of a GPAI model **integrates its own model into its own AI system** that is made available on the market / put into service, the obligation for GPAI models will continue to apply **in addition to those for AI systems**.
- Compliance with all of the above obligations must be **documented**.
- Providers of GPAI models, including GPAI models with systemic risk, may rely on **codes of practice** to demonstrate compliance with their obligations. The European Commission will launch the drafting of the first code of practice for GPAI models (including GPAI models with systemic risk) on September 30, 2024 and is aiming to have it ready **by April 2025**.
- If existing, Providers may also rely on **harmonized standards** or **common specifications** to demonstrate conformity.
- Providers bear an **obligation of cooperation** with competent authorities, which notably entails the obligation to provide all the information and documentation necessary to demonstrate compliance.
- Providers must **closely monitor regulatory developments** including any templates to be issued by the European Commission / AI Office.
- It is worth noting that **enforcement measures for GPAI models will become applicable one year after the deadline for compliance with the obligations**.



### Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



 [linkedin.com/showcase/ai-data-digital](https://www.linkedin.com/showcase/ai-data-digital)

### Contact us



**Anne-Gabrielle Haie**

Partner in Steptoe's AI, Data & Digital practice



## Obligations for Authorized Representatives of General-Purpose AI models

For a refresher on the notions of "Authorised Representative" and "General-Purpose AI model" (GPAI model), please consult our previous EU AI Act Decoded issues on "[Who will the EU AI Act apply to?](#)" and "[Classification of AI systems and GPAI Models](#)"

**Ensure that the appointment as Authorized Representative is made through a written mandate from the Provider**

(Art. 54)

- The written mandate must enable the Authorized Representative to perform all of the tasks assigned to it by the EU AI Act (detailed below).
- The written mandate must empower the Authorized Representative to be addressed, in addition to / instead of the Provider, by the AI Office or competent authorities on all issues related to compliance with the EU AI Act, and to provide them with all required information and documentation (incl. logs when relevant).

**Provide a copy of the written mandate to the AI Office upon request**

(Art. 54)

This must be provided in one of the official languages of the EU institutions.

**Verify Provider's compliance with the EU AI Act**

(Art. 54)

- The Authorized Representative must verify that the Provider has:
  - drawn up the technical documentation specified in Annex XI;
  - complied with all of its other obligations.

**Keep relevant documentation for 10 years after the placing on the EU market / putting into service of the GPAI model**

(Art. 54)

- The Authorized Representative must keep at the disposal of the AI Office and national competent authorities:
  - the Provider's contact details; and
  - a copy of the technical documentation.

**Terminate mandate if Provider is infringing the EU AI Act**

(Art. 54)

- ⚠ The Authorized Representative must terminate the mandate if it has reason to consider that the Provider is acting contrary to its obligations pursuant to the EU AI Act.
- ⚠ In such a case, the Authorized Representative must immediately inform the AI Office about the termination of the mandate and the reasons therefor.

### Notes:

- Authorized Representatives bear an **obligation of cooperation** with the AI office and competent authorities, which notably entails the obligation to provide all the information and documentation necessary to demonstrate compliance.



### Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



[in linkedin.com/showcase/ai-data-digital](https://www.linkedin.com/showcase/ai-data-digital)

### Contact us



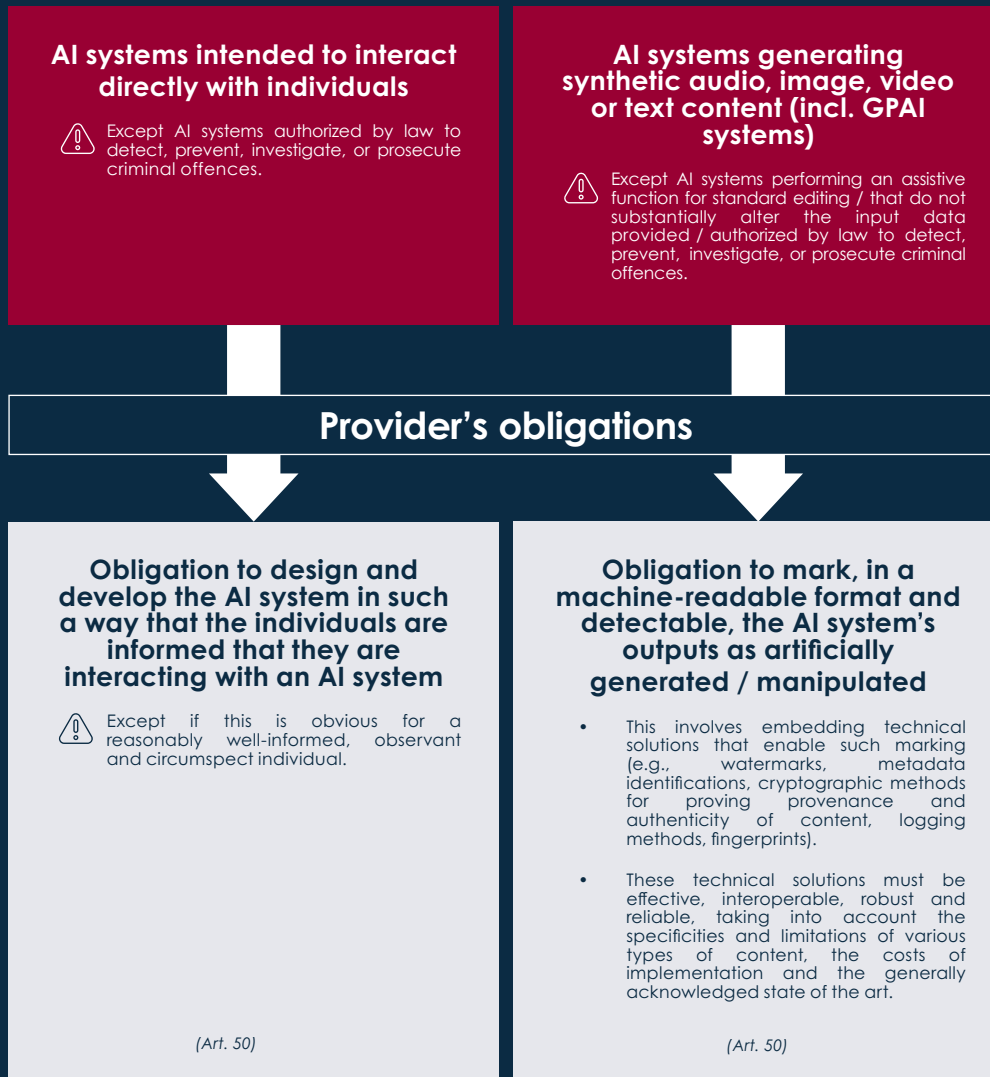
**Anne-Gabrielle Haie**  
Partner in Steptoe's AI,  
Data & Digital practice



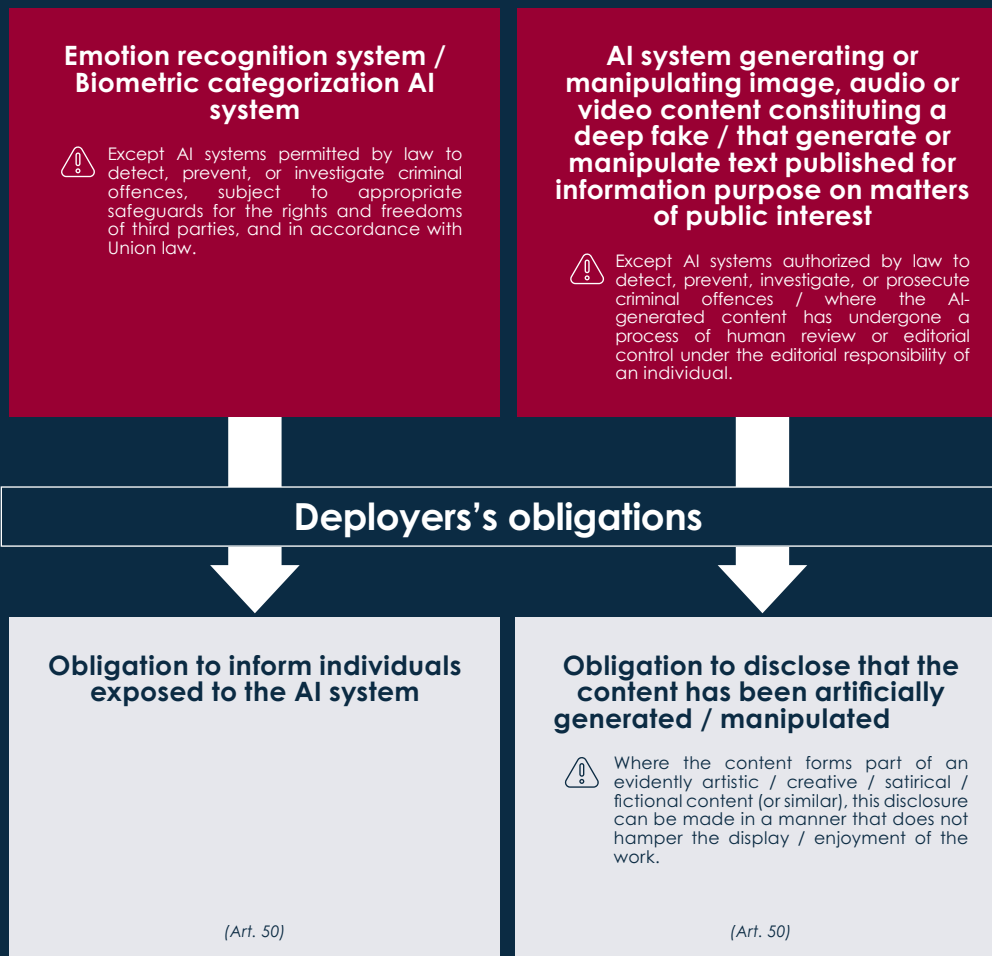
## Specific Transparency Obligations for Providers and Deployers of Certain AI Systems

For a refresher on the notions of “Provider”, “Deployer” and “AI systems subject to specific transparency obligations”, please consult our previous EU AI Act Decoded issues on “[Who will the EU AI Act apply to?](#)” and “[Classification of AI systems and GPAI Models](#)”.

### Concerned AI Systems



## Concerned AI Systems



**Deadline to comply with these obligations: August 2, 2026**

### Notes:

- These obligations intend to address potential **risks of impersonation or deception**, as well as **risks of misinformation and manipulation at scale, fraud, and consumer deception** posed by certain AI systems.
- These obligations may apply **in addition to the obligations imposed to high-risk AI systems**.
- The information must be provided in **a clear and distinguishable manner**, at the latest **at the time of the first interaction or exposure**. It must also conform to any applicable accessibility requirements.
- The EU AI Office is encouraged to facilitate the drawing-up of **codes of practice** at EU level in order to ensure the effective implementation of the obligations regarding the **detection and labelling of artificially generated or manipulated content**.



### Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



[in linkedin.com/showcase/ai-data-digital](https://www.linkedin.com/showcase/ai-data-digital)

### Contact us

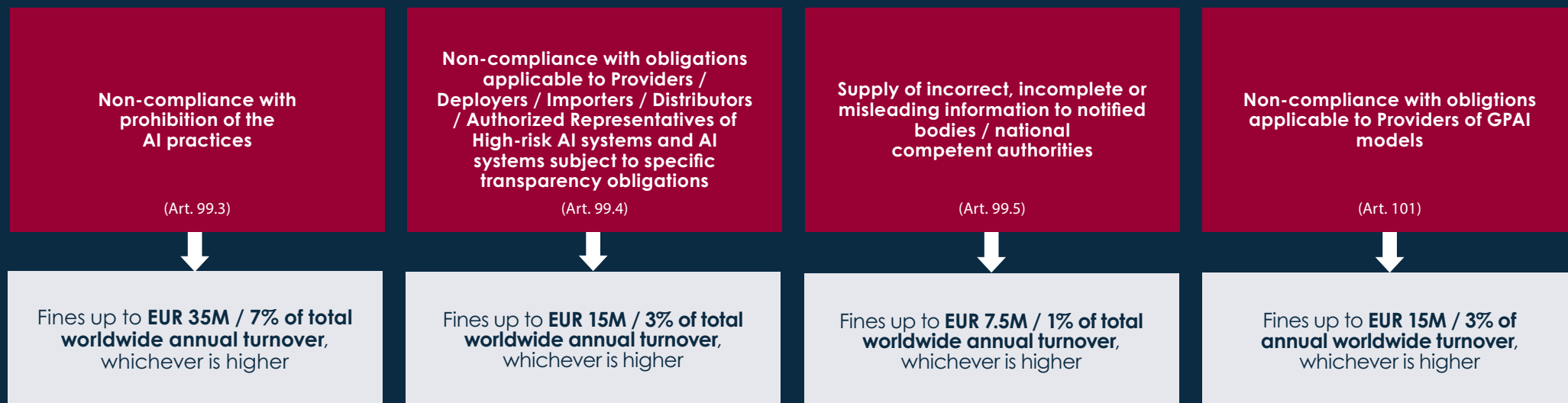


**Anne-Gabrielle Hale**  
Partner in Steptoe's AI,  
Data & Digital practice

# Steptoe | EU AI Act Decoded

## What Are the Risks in Case of Non-Compliance with the EU AI Act?

For a refresher on the notions of “Prohibited AI systems”, “High-risk AI systems”, “AI systems subject to specific transparency obligations”, “General-Purpose AI (GPAI) models”, “Provider”, “Deployer”, “Importer”, “Distributor”, “Authorized Representative”, please consult our previous EU AI Act Decoded issues on “[Classification of AI systems and GPAI Models](#)” and “[Who will the EU AI Act apply to?](#)”.



 **For SMEs (undertakings with < 250 employees, and an annual turnover ≤ EUR 50M / balance sheet ≤ EUR 43M), including start-ups, the applicable fine will be the lower amount.**

### Notes:

- Further rules on penalties and other enforcement measures (including warnings and non-monetary measures) will be determined by each EU Member State.
- The national market surveillance authorities and the AI Office are granted **extensive enforcement powers** to assess compliance with the EU AI Act. For high-risk AI systems and GPAI models, these powers notably include requiring providers to **provide full access to the documentation as well as the training, validation, and testing data sets used for development**, and, subject to certain conditions, **access to the source code**.
- Organizations are advised to monitor the regulatory developments in relation to the [Revised Product Liability Directive](#) (formally adopted on October 10, 2024) and the [Proposed AI Liability Directive](#) (still being discussed by the co-legislators). These Directives will introduce targeted reforms to national fault-based liability regimes and provide claimants with the right to request the disclosure of evidence to support their claims.



### Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



 [linkedin.com/showcase/ai-data-digital](https://www.linkedin.com/showcase/ai-data-digital)

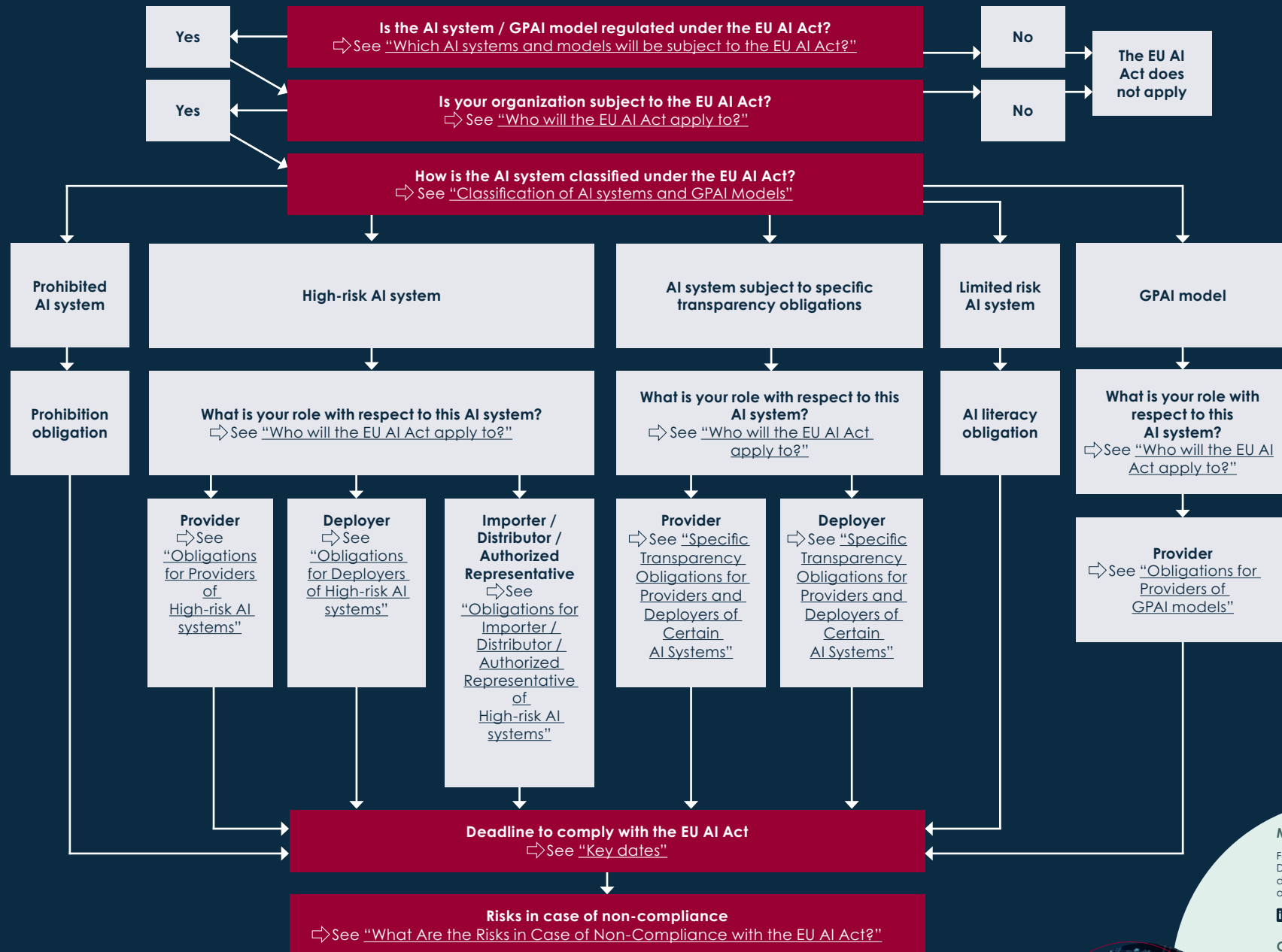
### Contact us



**Anne-Gabrielle Haie**  
Partner in Steptoe's AI,  
Data & Digital practice



# Steptoe | EU AI Act Decoded - Navigation Map



Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.

[in linkedin.com/showcase/ai-data-digital](https://www.linkedin.com/showcase/ai-data-digital)

Contact us



**Anne-Gabrielle Haie**  
Partner in Steptoe's AI, Data & Digital practice

## 10 steps to compliance

1

**Create an inventory of your AI systems / General-Purpose AI (GPAI) models and assess whether they fall within the scope of the EU AI Act**

- ✓ List and assess all of the AI systems / GPAI models that you develop / use / import / distribute
- ✓ Document your assessment
- ✓ Review regularly and maintain this inventory up-to-date

2

**Classify your AI systems / GPAI models**

- ✓ Check whether any exception applies (e.g., an AI system that could qualify as high-risk but does not pose a risk of harm to health, safety, or fundamental rights)
- ✓ Document your assessment
- ✓ Monitor any updates published by the European Commission
- ✓ Review regularly and maintain this assessment up-to-date

3

**Identify your role for each AI system / GPAI model and assess whether your organization is subject to the EU AI Act**

- ✓ Note that your organization can be subject to the EU AI Act despite being located or established outside of the EU
- ✓ Remember that your organization's role (e.g., Provider / Deployer) may be different depending on the AI system / GPAI model concerned
- ✓ Note that the qualification of your organization's role may change over time depending on what you do with the AI system / GPAI model
- ✓ Document the assessment of your organization's role for each AI system / GPAI model
- ✓ Regularly review this assessment and check whether it needs to be updated

4

**Map your obligations for each AI system / GPAI model**

- ✓ Make sure that you clearly identify your obligations for each AI system / GPAI model based on (i) its risk classification and (ii) your role
- ✓ Note that some documents must be specific to each AI system / GPAI model (e.g., technical documentation), while some policies, procedures, or measures could be common to all of your AI systems or GPAI models (e.g., AI literacy measures)
- ✓ Monitor templates and guidelines issued by the European Commission / AI Office / AI Board / national market surveillance authorities (collectively referred to as "regulators")
- ✓ Note that compliance with harmonized standards issued by standardization bodies or common specifications issued by the European Commission can help demonstrate compliance

5

**Identify any regulatory overlaps**

- ✓ Identify any regulatory overlaps and contradictions, particularly if you are active in a highly regulated sector (e.g., life sciences, financial sector, etc.)
- ✓ Document your assessment on why you believe that you are already complying with some of the EU AI Act's requirements in the context of your compliance with EU sector-specific laws
- ✓ Seek advice from competent authorities if you identify conflicting obligations or encounter any difficulties

6

### Prepare an inventory of existing documentation and processes, and conduct a gap analysis

- ✓ Inventory relevant existing documentation, procedures, and processes
- ✓ Conduct a gap analysis between what you already have in place and what is missing to comply with the EU AI Act
- ✓ Your organization is not starting from scratch! Build on what you have done thus far and enhance it

7

### Identify your internal resources and needs

- ✓ Set up a cross-department team
- ✓ Conduct a comprehensive evaluation of your available resources, including human, financial, and technical capabilities, that relate to your AI systems / GPAI models
- ✓ Identify training needs across your organization
- ✓ Identify areas where outside assistance / outsourcing may be needed
- ✓ Evaluate and anticipate your budget needs

8

### Prepare a roadmap and allocate responsibilities

- ✓ Having a game plan will help reduce the overwhelming feeling and meet deadlines
- ✓ Identify action points and organize them by priority
- ✓ Allocate responsibilities and set clear deadlines
- ✓ Maintain this roadmap up-to-date and track progress

9

### Monitor regulatory developments

- ✓ Monitor clarifications and guidance provided by regulators through guidelines, implementing regulations, templates, etc.
- ✓ Participate in consultation processes and workshops organized by regulators
- ✓ Keep abreast of the latest developments
- ✓ Monitor enforcement actions to understand regulators' priorities
- ✓ Engage with regulators

10


### Get involved in regulatory sandboxes, codes of practice, codes of conduct & standardization

- ✓ Monitor the establishment of, and participate in regulatory sandboxes across EU Member States
- ✓ Monitor and participate in the development of codes of practice
- ✓ Monitor and participate in the establishment of codes of conduct
- ✓ Monitor and participate in the development of standards prepared by standardization bodies

### Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



 [linkedin.com/showcase/ai-data-digital](https://www.linkedin.com/showcase/ai-data-digital)

### Contact us



**Anne-Gabrielle Haie**  
Partner in Steptoe's AI,  
Data & Digital practice



## Which authorities will be in charge of the enforcement and interpretation of the EU AI Act?



### AI Office

- **Supervision and enforcement** of rules related to **General Purpose AI (GPAI) models**.
- **Supports the implementation of rules on prohibited AI practices and high-risk AI systems** in coordination with relevant sectoral bodies.
- Issues **guidelines on practical implementation of the EU AI Act** (incl. templates).



### European AI Board

- Composed of 1 Representative per EU Member State + AI office which serves as secretariat of the Board (+ European Data Protection Supervisor as observer).
- **Advisory body** in charge of the **coordination and cooperation between national competent authorities** and of ensuring the **consistent implementation and application of the EU AI Act**.
- Issues **recommendations and opinions**.



### Scientific panel of independent experts

- Composed of **experts** selected by the European Commission **on the basis of up-to-date scientific or technical expertise in the field of AI**.
- **Advises and supports the AI Office with the implementation and enforcement of the EU AI Act as regards GPAI models and systems**.
- Supports the work of market surveillance authorities, at their request.



### Advisory Forum

- Composed of a balanced selection of stakeholders (incl. industry, start-ups, SMEs, civil society and academia).
- Provides **technical expertise and advice** the European AI Board and the AI Board.
- **May prepare opinions, recommendations and written contributions** at the request of the European AI Board and the AI Office.



### Notifying authorities

- At least 1 per EU Member State – To be designated by August 2, 2025.
- Responsible for setting up and carrying out the procedures for the assessment, designation and notification of **conformity assessment bodies and their monitoring**.



### Market surveillance authorities

- At least 1 per EU Member State => If several market surveillance authorities are designated, 1 will act as single point of contact – To be designated by August 2, 2025.
- **Supervision and enforcement** of rules related to **AI systems**.
- May provide **guidance and advice on the implementation of the EU AI Act**, taking into account the guidance and advice of the European AI Board and the AI Office.



### Authorities and bodies protecting fundamental rights

- **Supervision and enforcement** of obligations under **Union laws protecting fundamental rights** (incl. the right to non-discrimination) in relation to the **use of high-risk AI systems referred to in Annex III**.
- To be identified by November 2, 2024.

### Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.

[in linkedin.com/showcase/ai-data-digital](https://www.linkedin.com/showcase/ai-data-digital)

### Contact us



**Anne-Gabrielle Haie**  
Partner in Step toe's AI,  
Data & Digital practice

## What are the rights provided by the AI Act?

For a refresher on the notions of “High-risk AI systems”, “General-Purpose AI (GPAI) models”, “Deployer”, “Market Surveillance Authorities” please consult our previous EU AI Act Decoded issues on “[Classification of AI systems and GPAI Models](#)”, “[Who will the EU AI Act apply to?](#)” and “[Which authorities will be in charge of application and enforcement of the EU AI Act?](#)”.

### Right to explanation of individual decision-making (Art. 86)

- This right is recognized to any affected person who is subject to a decision taken by a Deployer of a High-risk AI system listed in Annex III mainly on the basis of the output of such system, and which decision:
  - o produces **legal effects**, or similarly,
  - o **significantly affects** that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights.
- It entails obtaining from the Deployer:
  - o **clear and meaningful** explanations of the role of the AI system in the decision-making procedure and
  - o the **main elements of the decision taken**, in a way that it serves as a foundation for the affected persons to exercise their rights.
- Affected persons **cannot exercise this right**:
  - o in relation to decisions taken pursuant to the output of high-risk AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity;
  - o when exceptions from or restrictions to this right follow from EU or national law; and
  - o overall, when it is otherwise provided under EU law.

### Right to lodge a complaint with a Market Surveillance Authority (Art. 86)

- This right entails that **any natural or legal person** that has grounds to consider that the EU AI Act has been infringed can submit complaints to the relevant Market Surveillance Authority.
- Such complaints **will be taken into account by Market Surveillance Authorities** for conducting their market surveillance activities, including investigations, in relation to the EU AI Act.

### Other administrative or judicial remedies (Art. 86)

**Any natural or legal person** whose rights and freedoms are adversely affected by the use of AI systems can pursue other administrative or judicial remedies available under EU or national law.

#### Notes:

- The rights provided by the EU AI Act are limited in comparison to those provided by other EU laws (e.g., GDPR).
- It is important to note that **the right to lodge a complaint is available to both natural and legal persons**. Furthermore, **no specific interest or legal standing appears to be required**, as the EU AI Act only refers to suspicions of non-compliance without mandating the demonstration of any damage to justify the complaint. In practice, **this right could potentially be used by a company against its competitors**.
- Persons acting as **whistleblowers on infringements of the EU AI Act are protected** under the EU Directive 2019/1937 ([Whistleblowing Directive](#)) in relation to the reporting of such infringements.



#### Much more to explore!

Follow our EU AI Act Decoded Series as we delve into the intricacies of the EU AI Act.



[linkedin.com/showcase/ai-data-digital](https://www.linkedin.com/showcase/ai-data-digital)

#### Contact us



**Anne-Gabrielle Haie**  
Partner in Step toe's AI,  
Data & Digital practice

