Steptoe | **EU AI Act Decoded**

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 a 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 the 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 EU 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 the 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 covered by Annex III, 1. (a).

Design the 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 the 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 / 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 / the environment in which it operates, in particular due to its interaction with individuals / 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 EU market / put into service;
- ensure **resiliency against attempts by unauthorized third parties** to alter its 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 EU market / the putting into service of the 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 EU 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 EU 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 EU 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 the 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 AI system has been placed on the EU 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 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 EU market / putting into service. The provider / its authorized representative must also register itself.

⚠ 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 EU 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 February 2, 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 / 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 the 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 of 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 spam **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 these other EU laws**.
- 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

Contact us

Anne-Gabrielle Haie

Partner in Steptoe's AI, Data & Digital practice