Steptoe | **EU AI Act Decoded**

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** 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 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 t**he 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 element 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 (DPIA) 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.

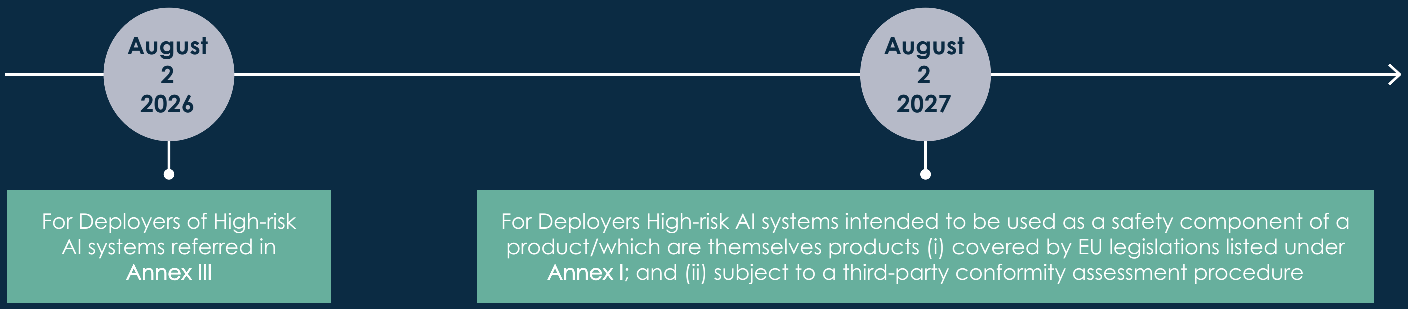
⚠ The AI Office will develop a template questionnaire to conduct FRIA.

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 the 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

Contact us

Anne-Gabrielle Haie

Partner in Steptoe's AI, Data & Digital practice