If you cannot see this email, please click here_

Luxembourg Newsflash - 22 March 2024

EU Parliament adopts final version of AI Act:our key takeaways

The first comprehensive ai regulation in the world aims for strong protection against harmful impacts.

Reading time: 9 minutes, 45 seconds

1. Context

After much anticipation, the EU Parliament formally adopted the final version of the proposal for an EU regulation laying down harmonised rules on artificial intelligence (AI Act) [1] on 13 March 2024. The text is still subject to a final lawyer-linguist check and needs to be formally endorsed by the Council of the EU.

Initially proposed by the EU Commission in April 2021, the proposal has been amended over the years to take account of technological developments, particularly generative AI and the launch of ChatGPT in November 2022.

The AI Act is the first comprehensive regulation for the artificial intelligence (AI) industry worldwide. It aims to ensure a high level of protection from harmful effects of AI systems in the EU, while supporting innovation and improving the functioning of the internal market.

The AI Act seeks to provide all market players with clear requirements and obligations regarding specific uses of AI. Accordingly, it sets out directly applicable rules on the development, marketing, commissioning and use of AI systems within the EU. It also applies more generally to machine learning training, testing and validation datasets.

2. Key features of the AI Act

Here are our main takeaways about the AI Act:

1. Definitions

- **Broad definition of "AI system":**

"A machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".

This definition is intentionally broad to remain “technologically neutral” and thus ensure that the text will not become outdated given this ever-evolving technology.

- **Dual definition of “high-risk AI systems”:**

An AI system will be considered high-risk if it satisfies either of the following two conditions:

- The AI system (i) **is a product (or is intended to be used as a safety component of a product) covered by specific EU legislation listed in Annex II of the AI Act** (e.g. civil aviation, vehicle security, toys, marine equipment, lifts, personal protective equipment and medical devices); and (ii) **is required to undergo a third-party conformity assessment, with a view to the placing on the market or putting into service of that product pursuant to such specific legislation.**

- **It is on the list of AI systems in Annex III of the AI Act** (e.g. remote biometric identification systems, critical infrastructure, education and vocational training, employment, worker management, access to and enjoyment of essential private services and essential public services and benefits, law enforcement, administration of justice and democratic processes).

High-risk AI systems are subject to more stringent regulation than those that are lower risk.

- **Specific definition of "General purpose AI model”:**

“An AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This does not cover AI models that are used before release on the market for research, development and prototyping activities”.

General purpose AI (GPAI) models are treated differently, given the potentially significant risks associated with their development and deployment (see point iii below).

2. Risk-based approach

- The AI Act applies a **tiered approach based on how risky AI applications are deemed to be.** “Risk” is defined as “the combination of the probability of an occurrence of harm and the severity of that harm”.

- On that basis:

    - **Unacceptable AI practices** are banned in the EU. These include manipulative AI, social scoring systems, real-time remote biometric identification systems in public spaces for law enforcement purposes (limited exceptions may apply under very strict conditions) and inferring emotions in workplaces or educational institutions, other than for medical or safety reasons.

    - **High-risk AI systems** are subject to extensive and burdensome obligations, including implementation of appropriate technical and organisational measures, human oversight, exercise of control, monitoring, keeping automatically generated logs and assessing impact on fundamental rights.

    - **Lower risk AI systems** must comply with transparency requirements. Providers are obliged to ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system. Deployers are also required to make certain disclosures, in particular in the case of generation or manipulation of content. Those disclosures must be done in a clear and distinguishable manner at the latest at the time of the natural person’s first interaction with or exposure to the AI system.

3. General purpose AI models

Under the AI Act, models are regulated separately from AI systems.

GPAI models are classified depending on their risk. A GPAI model will be characterised as "with systemic risk" if it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks (or the EU Commission has decided that a GPAI model has equivalent capabilities or impact).

Providers of GPAI models are subject to specific obligations such as:

- drawing up and maintaining the model's technical documentation;
- making information and documentation available to providers of AI systems who intend to integrate the GPAI model into their own AI system; and
- putting in place a policy to comply with EU copyright law.

Additional obligations apply to providers of GPAI models with systemic risk, including assessment and mitigation of the systemic risk and ensuring an adequate level of cybersecurity protection.

4. Obligations throughout the value chain, particularly for deployers (users)

The AI Act imposes obligations throughout the entire value chain: from providers, importers and distributors to deployers of AI solutions within the EU, as well as persons adversely impacted by the use of an AI system placed on the market or put into service in the EU.

A deployer is "any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity".

All Luxembourg companies, whether or not regulated, may come within the scope of the AI Act's requirements to some extent as soon as they are in contact with an AI system (i.e. as deployer of the AI system). The relevant requirements (e.g. transparency, policies and procedures, notification to authorities) will differ, depending on both their own characterisation within the meaning of the AI Act, and on the level of risk of the AI system(s) concerned.

In particular, specific transparency obligations will apply when using:

- an emotion recognition or biometric categorisation system;
- an AI system that generates or manipulates image, audio or video content constituting a deep fake; or
- an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest.

Certain entities (banks [2], insurers [3] and public services) will have to carry out a fundamental rights impact assessment prior to deploying a high-risk AI system.

5. AI regulatory sandboxes

"AI regulatory sandboxes… provide for a controlled environment that fosters innovation and facilitates the development, training, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific sandbox plan agreed between the prospective providers and the competent authority."

The AI Act requires national competent authorities to establish at least one AI regulatory sandbox at national level, which must be operational 24 months after the AI Act enters into force. The sandbox may also be established jointly with one or several other Member States' competent authorities. The EU

Commission may provide technical support, advice and tools for the establishment and operation of AI regulatory sandboxes.

Competent authorities will have to provide, as appropriate, guidance, supervision and support within the sandbox with a view to identifying risks, in particular to fundamental rights, health and safety, testing, mitigation measures, and their effectiveness in relation to the obligations and requirements of the AI Act and, where relevant, other EU and Member States legislation supervised within the sandbox.

6. Governance

- **AI Office**: the EU Commission will establish the European AI Office to develop EU expertise and capabilities in the field of AI.

- **EAIB**: the AI Act establishes a "European Artificial Intelligence Board" composed of one representative per Member State. The European Data Protection Supervisor (EDPS) will participate as observer and the AI Office will also attend without taking part in the votes. The EAIB will advise and assist the EU Commission and the Member States in order to facilitate the consistent and effective application of the AI Act.

- **Advisory forum**: the AI Act establishes an advisory forum to advise and provide technical expertise to the EAIB and the EU Commission to contribute to their tasks under the AI Act. The membership of the advisory forum must represent a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society and academia.

- **Scientific panel**: the EU Commission will establish a scientific panel of independent experts (selected by the EU Commission on the basis of up-to-date scientific or technical expertise in the field of AI) intended to support the enforcement activities under the AI Act. Member States may call upon experts on the scientific panel to support their enforcement activities under the AI Act.

- **National competent authorities**: each Member State must establish or designate at least:

    - **One notifying authority**

    - **One market surveillance authority**

Their identity and tasks must be notified to the EU Commission. The EDPS has been designated as the competent authority for the supervision of EU institutions, agencies and bodies falling within the scope of the AI Act.

- **EU database for high-risk AI systems listed in Annex III**: the EU Commission (in collaboration with Member States) will set up and maintain an EU database containing information concerning certain high-risk AI systems.

7. Sanctions

Market surveillance authorities will be able to impose sanctions in cases of non-compliance with the AI Act. These will include fines of up to 35 million euros or, if the offender is a company, up to 7% of its total worldwide annual turnover in cases of prohibited AI practices.

For providers of GPAI, the EU Commission may impose fines of up to 15 million euros or 3% of total worldwide turnover in the preceding financial year, whichever is higher.

The supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request will also be subject to administrative fines of up to 7.5 million euros or, if the offender is a company, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

8. Other requirements

Obviously, it is also essential to address issues such as intellectual property, data protection, regulatory requirements, cybersecurity, contracts and liability to ensure responsible AI deployment.

As AI technologies continue to evolve, alignment with legal standards becomes increasingly important to mitigate risks and promote trust in AI-driven systems.

What's next?

The adoption of the AI Act marks a significant milestone in shaping the future of AI governance. Once published in the Official Journal of the EU, the AI Act will enter into force on the 20th day following its publication. It will generally become fully applicable 24 months after its entry into force.

However, certain specific timelines will apply from the entry into force of the text:

- **6 months**: enforcement of prohibited systems will start to apply
- **9 months**: provisions relating to codes of practice
- **12 months**: GPAI rules will take effect (except for GPAI models placed on the market before this date which will be granted an additional delay of 24 months)
- **36 months**: obligations for high-risk systems

How we can help

Contact our experts in the **IP, Communication & Technology Team** (ip_it_dataprotectionteam@arendt.com) and **Regulatory & Consulting** for further assistance on how to comply with the AI Act. They will be delighted to support you in scoping the AI Act's applicability in your specific business context, and to assist with the required compliance actions.

[1] Interinstitutional File: 2021/0106(COD).

[2] For "AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud".

[3] For "AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance."

your contacts

IP, Communication & Technology

ASTRID WAGNER
Partner
Learn more_

FAUSTINE CACHERA
Senior Associate
Learn more_

SOPHIE CALMES
Senior Associate
Learn more_

JULIEN PÉTRÉ
Senior Associate
Learn more_

Regulatory Consulting

YANN FIHEY
Partner

Learn more_

BÉNÉDICTE D'ALLARD
Senior Manager

Learn more_

DELPHINE GARNIER
Manager

Learn more_

Arendt & Medernach SA
Registered with the Luxembourg Bar
RCS Luxembourg B 186371

arendt.com

41A avenue JF Kennedy
L-2082 Luxembourg
T +352 40 78 78 1