

**C L I F F O R D**

**C H A N C E**

**THE EU AI ACT**  
**OVERVIEW OF KEY RULES AND REQUIREMENTS**

# CONTENTS

## Scoping

1. When will the requirements of the AI Act start applying? 3
2. What technology does the AI Act apply to? 4
3. Does the AI Act only affect EU businesses? 5
4. What types of operators are affected by the AI Act? 5
5. How does the AI Act take account of sectoral specificities? 5

## Assessing requirements

6. What are the AI literacy requirements that apply to businesses? 6
7. What practices are prohibited under the AI Act? 7
8. What AI systems are considered high-risk? What is the 'filter system'? 7
9. What are the requirements for high-risk AI systems? 8
10. Who must conduct a fundamental rights impact assessment? 10
11. What rules apply to GPAI models? 10
12. What are the specific transparency requirements for certain AI? 12
13. What about the general core principles that were envisaged for all AI systems? 12

## Looking forward

14. How will the AI Act be enforced? What fines will apply? 13
15. What secondary legislation and guidance are we expecting going forward? 14

## THE EU AI ACT OVERVIEW OF KEY RULES AND REQUIREMENTS

On 12 July 2024, the EU Artificial Intelligence Act (AI Act) was finally published in the EU's Official Journal<sup>1</sup>, marking the conclusion of a long elaboration and adoption process.

The EU AI Act will now enter into force on 1 August 2024, and the first of its requirements to kick in will start to apply very soon afterwards – i.e., on 2 February 2025.

This document highlights some of the key points to note.

### Scoping

#### 1. When will the requirements of the AI Act start applying?

The entry into application of the AI Act will be gradual, with different transition periods following entry into force for different requirements. For instance:

**2 February 2025:** Prohibitions, AI literacy, general provisions

**2 August 2025:** General-purpose AI, provisions on Member State penalties

**2 August 2026\*:** Standalone high-risk AI (e.g. life/health insurance risk assessment, credit scoring, HR), specific transparency requirements, regulatory sandboxes, etc.


\*By-default transition period


**2 August 2027:** High-risk AI under specific sectoral legislation (e.g., re medical devices, radio equipment, toys, machinery), general-purpose AI models already on the market


Also, further transition periods will in fact apply:

- (a) **Fines:** Whilst the prohibitions kick in on 2 February 2025, the provisions on penalties and fines in principle only start to apply later. Further, although requirements for providers of general-purpose AI (“**GPAI**”) models become applicable on 2 August 2025, related fines in principle only start applying after a further 12 months.
- (b) **Systems or models already on the market:** There are for instance specific rules to address pre-existing high-risk AI systems and GPAI models:
  - Operators of pre-existing high-risk AI systems will need to comply with the AI Act's requirements if those high-risk systems are subject to significant changes in their design after the date the requirements for high-risk AI systems under the AI Act start to apply<sup>2</sup>; and

### What's next for businesses?

 Ramp up awareness.

 Set up and deploy a realistic implementation plan with due priorities.

 Onboard key stakeholders.

This paper aims at helping you navigate some of the complexities of the AI Act and hopefully assisting you with your awareness raising efforts.

<sup>1</sup> Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) – Text with EEA relevance. Please see here: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

<sup>2</sup> With further specificities for providers and deployers of high-risk AI systems intended to be used by public authorities.

- Providers of GPAI models placed on the market before 2 August 2025 will need to take the necessary steps to comply by 2 August 2027 (i.e. 36 months following the entry into force of the AI Act).

## 2. What technology does the AI Act apply to?

The AI Act has a broad scope, regulating the placing on the market, putting into service and use of AI across sectors on a horizontal basis. This is reflected in the **notion of AI system itself**, which aims to be as technology and future-proof as possible and to align with the work of international organisations, and in particular that of the OECD.

Whilst the notion is broad, the objective is nonetheless to distinguish AI systems from simpler traditional software or programming approaches, and to ensure the definition doesn't for instance capture pure automation<sup>3</sup>. Key characteristics of the notion include, amongst other things:

- (a) **The capability to infer**<sup>4</sup> how to generate outputs that can influence physical or virtual environments.
- (b) **Running on machines.**
- (c) Having some **degree of independence of actions from human involvement** and of capabilities to operate without human intervention.

Another key notion is the concept of **GPAI model**. These are AI models displaying significant generality, which can perform a wide variety of tasks across multiple domains and contexts and can be integrated into a variety of downstream systems or applications<sup>5</sup>. A prime example of a GPAI model is a large generative AI model.

Also, some AI systems or models will fall outside the scope of the AI Act. This is the case for instance of AI systems placed on the market, put into service or used exclusively for military, defence or national security purposes. This is also the case of AI systems and models, including their output, specifically developed and put into service for the sole purpose of scientific research and development. There are also exclusions / specific rules with respect to certain AI systems (or tools, services, components, or processes used or integrated in a high-risk AI system), or GPAI models, released under free and open-source licences. However, they are very specific and subject to conditions / exceptions. As a general rule, exceptions may be tricky to apply and need to be carefully considered.

<sup>3</sup> Meaning here systems based on rules defined solely by natural persons to automatically execute operations.

<sup>4</sup> e.g. based on techniques such as "machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved".

<sup>5</sup> More specifically, a GPAI model is defined as "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". As per the AI Act: "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, such as for example a user interface, to become AI systems. AI models are typically integrated into and form part of AI systems. (...)".

### 3. Does the AI Act only affect EU businesses?

#### EU-based

- Providers established or located in the EU that place on the market or put into service AI systems, or place on the market GPAI models, in the EU.
- Deployers established or located in the EU.
- Authorised representatives, importers established or located in the EU, etc.

**No. It will have a global reach and can affect both EU and non-EU-based businesses, e.g:**

The key question is the effect on the EU, and not necessarily where the relevant operator is based.

#### Not EU-based

- Third country providers placing on the market or putting into service AI systems, or placing on the market GPAI models, in the EU.
- Providers and deployers of AI systems having their place of establishment or located in a third country where the output produced by the AI system is used in the EU<sup>6</sup>.

### 4. What types of operators are affected by the AI Act?

The AI Act imposes obligations on operators across the entire AI value chain.

Whilst the most stringent obligations apply to providers (including downstream providers), specific obligations also apply to downstream operators including deployers, importers and distributors – each as defined in the AI Act. There are also requirements impacting suppliers of AI systems, tools, services, components or processes that are used or integrated in a high-risk AI system.

The qualification of an operator's role under the AI Act is key to ascertain the applicable rules and responsibilities, and it requires a clear understanding of each role.

Moreover, deployers, distributors, importers and other third parties will be deemed the provider of a high-risk AI system, and will assume the related legal responsibilities, where they (a) put their name or trademark on a high-risk AI system already on the market or in service, (b) make a 'substantial modification' to a high-risk AI system already on the market or in service and it remains high-risk, or (c) modify the 'intended purpose' of an AI system, including a GPAI system, in such a way that it becomes high-risk.

In situations where operators act in more than one capacity at the same time, they will need to fulfill cumulatively all relevant obligations associated with those roles.

### 5. How does the AI Act take account of sectoral specificities?

One of the concerns voiced in relation to the AI Act, from early on, is the interplay, and risk of overlap or conflict, with other rules, in particular in sectors that are heavily regulated.

<sup>6</sup> AI Act, Recital 22: "(...) In light of their digital nature, certain AI systems should fall within the scope of this Regulation even when they are not placed on the market, put into service, or used in the Union. This is the case, for example, where an operator established in the Union contracts certain services to an operator established in a third country in relation to an activity to be performed by an AI system that would qualify as high-risk. In those circumstances, the AI system used in a third country by the operator could process data lawfully collected in and transferred from the Union and provide to the contracting operator in the Union the output of that AI system resulting from that processing, without that AI system being placed on the market, put into service or used in the Union. To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and deployers of AI systems that are established in a third country, to the extent the output produced by those systems is intended to be used in the Union".

The AI Act takes account of sectoral specificities in different ways, e.g. and in addition to the exclusions above:

- (a) **Impacting sectoral legislation:** For AI systems that qualify as high-risk under the AI Act because they are products, or intended to be used as safety components of products, covered by specific sectoral legislation (in particular, in the fields of civil aviation, two or three-wheel vehicles and quadricycles, agricultural and forestry vehicles, marine equipment, the interoperability of the rail system, or motor vehicles), only a limited number of the AI Act's provisions will be directly applicable through the AI Act.

On the other hand, the requirements of the AI Act regarding high-risk AI systems are to be taken into account under the relevant sectoral legislation, in particular when adopting related delegated or implementing acts, technical specifications or testing standards on the basis of that legislation, and that legislation is amended accordingly.

- (b) **Cross-compliance:** In certain circumstances, obligations under the AI Act may be deemed fulfilled by complying with related requirements under relevant sectoral legislation.

A notable example relates to financial services. For instance, if a provider is a financial institution that is already subject to requirements regarding its internal governance or processes under EU financial services law, its obligation to put in place a quality management system under the AI Act should be considered met, at least for part of the requirements, by complying with the rules pursuant to the relevant EU financial services law.

- (c) **Longer transition period:** The requirements for some AI systems that qualify as high-risk AI systems due to their being products, or safety components of products, under specific sectoral legislation start applying later<sup>7</sup>.

- (d) **Guidelines:** The European Commission is tasked with issuing guidelines to help navigate the relationship between the AI Act and sector-specific laws, including as regards consistency in enforcement.

The interplay between the AI Act and sectoral rules is likely to be a critical focus area as we turn to the implementation and enforcement of the AI Act, with calls for measures to facilitate that implementation together with applicable sectoral regulations and avoid unnecessary administrative burdens and overlaps. Issues and complexities have already surfaced.

## Assessing requirements

### 6. What are the AI literacy requirements that apply to businesses?

Providers and deployers of AI systems will need to take measures to ensure a sufficient level of 'AI literacy' of their staff and others involved in the operation and use of AI systems on their behalf. This entails ensuring appropriate skills, knowledge and understanding, taking account of respective rights and obligations under the AI Act, for an informed deployment of AI systems, as well as awareness of the opportunities and risks of AI and possible harm it can cause.

There is some uncertainty concerning the AI literacy requirements, which are amongst the first to apply, in particular as regards their precise scope and implementation.

In practice, this will notably translate into awareness raising campaigns and training.

<sup>7</sup> See section 8(a)(i) below, and the implementation timeline above.

## 7. What practices are prohibited under the AI Act?

There are currently eight types of prohibited practices. Compared to the European Commission's initial proposal in 2021, the final list has been expanded to also cover, amongst other things, the placing on the market, putting into service or use of:

- (a) AI systems for **social scoring** by both public and private actors, and not only by or on behalf of public authorities as initially envisaged.
- (b) AI systems to **infer emotions in the areas of workplace and education institutions**.
- (c) AI systems that **create or expand facial recognition databases through the untargeted scraping of facial images** from the internet or CCTV footage.
- (d) AI systems linked to **assessing or predicting the risk of a natural person committing a criminal offence, based solely on profiling or assessing personality traits and characteristics**.
- (e) **Biometric categorisation systems** that categorise individually natural persons **based on their biometric data to deduce or infer** race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.

Other prohibited practices relate to: the **deployment of subliminal, manipulative or deceptive techniques; the exploitation of vulnerabilities** due to age, disability or a specific social or economic situation; the use of **real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes**.

There are additional conditions and/or exceptions for the prohibited practices, and an in-depth assessment is required to ensure compliance with the AI Act.

## 8. What AI systems are considered high-risk? What is the 'filter system'?

- (a) **Notion:** There are **broadly two categories** of high-risk AI systems under the AI Act:
  - (i) The first refers to AI systems that are products, or safety components of products, that **come under specific sectoral legislation and are subject to a third-party conformity assessment pursuant to that legislation** with a view to placing on the market or putting into service.

This category may include (a) cars, aircraft including as regards unmanned aircraft and other items coming under the specific sectoral legislation mentioned in section 5(a) above, as well as (b) machinery, toys, lifts, radio equipment, medical devices and in vitro diagnostic medical devices, amongst others.
  - (ii) The second category refers to a list of **'standalone' high-risk AI systems** currently coming within one of eight areas<sup>8</sup>. The list covers various different AI use cases, including for instance AI systems intended to be used for:
    - **HR purposes**, e.g. for recruitment or selection, to make decisions affecting terms of work-related relationships, promotion or termination of work-related contractual relationships, to allocate tasks based on behaviour or personal traits, to monitor and evaluate performance.
    - **Evaluating creditworthiness or establishing credit score** (except systems used to detect financial fraud).
    - **Risk assessment and pricing in relation to natural persons re life and health insurance**.

<sup>8</sup> AI Act, Annex III.

- **Remote biometric identification, biometric categorisation according to sensitive or protected characteristics based on their inference or emotion recognition**, to the extent not prohibited.
- **Education and vocational training**, e.g. for determining admission to institutions or evaluating learning outcomes.
- **Safety components in the management and operation of critical digital infrastructure**.

(b) **Filter system:** An AI system coming within the ‘standalone’ high-risk AI systems could nonetheless not be considered as high-risk if, in the circumstances, it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision-making. This could be the case if one or more of the following criteria are met, with the recitals providing illustrations:

- The AI system is intended to perform a narrow procedural task.
- The AI system is intended to improve the result of a previously completed human activity.
- The AI system is intended to detect decision-making patterns or deviations from previous patterns and is not meant to replace or influence the previously completed human assessment, without proper human review.
- The AI system is intended to perform a preparatory task to an assessment relevant for a high-risk use case under Annex III.

There is a general safeguard for systems involving profiling, however. An AI system used in a high-risk use case listed in Annex III will in any event be considered high-risk if it performs profiling, notwithstanding the filter system.

The filter system relies on a documented self-assessment by the provider, and it requires prior registration in an EU database. If the provider uses the filter system to circumvent the AI Act, it exposes itself to substantial fines.

(c) **The AI Act, and beyond:** The AI Act itself emphasises and serves as a reminder that the AI Act cannot be viewed in isolation. For instance, it stresses that the classification of an AI system as high-risk under the AI Act does not necessarily mean that its use is lawful under other rules.

## 9. What are the requirements for high-risk AI systems?

Specific obligations apply to high-risk AI systems, and these differ based on the operator’s role.

For instance, providers of high-risk AI systems are subject to a broad set of requirements in terms e.g. of risk and quality management, data governance including to prevent bias, documentation and record-keeping, transparency, registration, human oversight, accuracy, robustness and cybersecurity, and conformity assessments. They include, amongst other things:

- **Implementing risk and quality management systems:** Providers of high-risk AI systems must develop a risk management system that is run and regularly reviewed and updated throughout the AI system’s entire lifecycle. It includes identifying and analysing both known and reasonably foreseeable risks related to health and safety and fundamental rights, and adopting appropriate and targeted risk management measures



to address relevant risks that are identified. It also involves testing to determine the most appropriate and targeted risk management measures.

That risk management system is part of the quality management system that providers of high-risk AI systems must put in place, to ensure compliance with the AI Act. The quality management system must be documented in written policies, procedures and instructions, and include key aspects such as: a strategy for regulatory compliance; systematic actions for the design, design control and design verification of the AI system, as well as for its development, quality control and quality assurance; examination, test and validation procedures; systems and procedures for data management; a post-market monitoring system; procedures for the reporting of serious incidents; security-of-supply related measures; and an accountability framework setting out the responsibilities of the management and other staff.

- **Implementing data governance measures and ensuring the quality of datasets:**

Training, validation and testing datasets used in relation to high-risk AI systems need to be relevant, sufficiently representative, and – to the best extent possible – free of errors and complete in view of the system’s intended purpose. They also need to have the appropriate statistical properties, including as regards the persons or groups of persons in relation to whom the system is intended to be used.

Specifically on the critical issue of bias, datasets need to be examined in view of possible biases; and appropriate measures need to be implemented to detect, prevent and mitigate biases that may have been identified.

- **Enabling appropriate human oversight:** High-risk AI systems must be designed to allow for effective human supervision, including the capability to halt system operations immediately if necessary. Different types of oversight measures are envisaged: those that are built into the AI system by the provider before it is placed on the market or put into service, and those that are identified by the provider before that time and that are appropriate to be implemented by the deployer. The high-risk AI system must be provided to the deployer in such a way that the people to whom human oversight is assigned can, amongst other things and as appropriate, properly understand its capacities and limitations, monitor its operation, interpret its output, decide not to use it, disregard its output and safely halt it e.g. through a stop button.

There is a flow-down of responsibilities along the value chain, with other operators being subject to specific requirements too. As regards deployers, many are correlated to those of the provider, and include:

- **Complying with instructions for use:** Deployers must take appropriate technical and organisational measures to ensure they use the high-risk AI systems in accordance with the provider’s instructions for use.
- **Ensuring the relevance of input data:** Deployers must ensure that the input data is relevant and sufficiently representative, where they have control over it.
- **Properly assigning human oversight:** Deployers must ensure they assign human oversight to people having the necessary competence, training and authority, as well as the requisite support.
- **Monitoring the AI system:** Deployers must monitor the operation of the high-risk AI system in accordance with the instructions for use, provide relevant information to other operators and authorities as applicable in case of incidents, and suspend the use of the AI system in certain cases.

- **Providing information to affected people:** There are important transparency requirements for deployers, aside from the specific requirements mentioned in section 12. For instance, deployers of ‘standalone’ high-risk AI systems that make or assist in making decisions related to natural persons must inform the latter that they are subject to the use of the system. In the field of HR, deployers who are employers must, before putting into service or using a high-risk AI system at the workplace, inform workers’ representatives and the affected workers that they will be subject to the use of the system. Where applicable, this information is to be provided in accordance with EU and national rules, procedures and related practice on information of workers and their representatives.

Some operators are also required to carry out a fundamental rights impact assessment.

## 10. Who must conduct a fundamental rights impact assessment?

An important discussion point during the AI Act trilogues was the European Parliament’s proposal to impose a requirement on deployers to carry out a fundamental rights impact assessment (“**FRIA**”) prior to putting a high-risk AI system into use. The requirement will be more limited than initially proposed, and it will apply to the following:

- (a) **Concerned AI systems:** A high-risk AI system, coming within the ‘standalone’ high-risk AI systems of Annex III, except those used in the management and operation of critical infrastructure.
- (b) **Concerned operators:** A deployer that is:
  - A body governed by public law, or a private operator providing public services.
  - An operator deploying a high-risk AI system (i) to evaluate the creditworthiness of natural persons or establish their credit score, or (ii) for risk assessment and pricing in relation to natural persons in the case of life and health insurance.

The FRIA will basically require deployers, prior to deploying the relevant high-risk AI system, to conduct an impact assessment, which will include: a description of the deployer’s processes in which the AI system will be used; the categories of persons / groups likely to be affected; the specific risks of harm likely to have an impact on them; a description of the implementation of human oversight measures, according to the instructions for use; and measures to be taken if those risks materialise including governance arrangements e.g. for human oversight, or complaint handling and redress procedures.

## 11. What rules apply to GPAI models?

As was anticipated, the AI Act provides a specific framework for the regulation of GPAI models. It includes a series of requirements for providers of all GPAI models, and additional requirements for providers of those with systemic risk. This is one of the areas that has seen the most significant developments compared to the European Commission’s initial proposal in 2021. Here are key aspects of this framework:

### (a) Rules for all GPAI models

- Providers of GPAI models will have to comply with specific requirements. As per our key takeaways on the AI Act political agreement of December 2023<sup>9</sup>, these include rules around: (i) technical documentation; (ii) information to be made available to providers of AI systems intending to integrate the GPAI model into their AI systems, and enabling them to have a good understanding of the model’s capabilities and

<sup>9</sup> See here: [The EU’s AI Act. What do we know about the critical political deal?](#)

limitations and to comply with the AI Act; (iii) a policy to respect EU law on copyright and related rights, in particular to identify and comply with reservations of rights expressed by rightsholders with respect to reproductions and extractions for text and data mining pursuant to the EU Directive on copyright and related rights<sup>10</sup>; (iv) a sufficiently detailed summary re the content used for training of the model, based on a template to be provided by the AI Office; (v) cooperation with the relevant authorities. There are also particular provisions re the designation of authorised representatives, where the provider is established outside the EU, in relation specifically to GPAI models. Some of the requirements will not apply, however, where the AI models are made accessible under a free and open-source licence unless they are GPAI models with systemic risks.

- The European Commission will have exclusive powers regarding the supervision and enforcement of the provisions regarding GPAI models, entrusting these tasks to the AI Office.
- Codes of practice and harmonised standards need to be developed, and secondary legislation needs to be adopted under the AI Act.

**(b) Additional rules for GPAI models with systemic risk<sup>11</sup>**

- A GPAI model will be classified as having systemic risk if:
  - It has 'high impact capabilities' – this means capabilities that match or exceed those recorded in the most advanced GPAI models – evaluated based on appropriate technical tools and methodologies; or
  - It has equivalent capabilities / impact having regard to specific criteria, based on a decision of the European Commission. Criteria include such things as the model's number of parameters, quality or size of the data set, amount of computation used for training, input and output modalities, model capabilities including level of autonomy and scalability or tools the model has access to, impact on the internal market due to reach (with a presumption of high impact where it is made available to at least 10,000 registered business users established in the EU), number of registered end users.
- A GPAI model is presumed to have high impact capabilities, and therefore to present systemic risks, when the cumulative amount of computation used for its training measured in floating point operations is greater than  $10^{25}$ .
- Providers of GPAI models qualifying as GPAI models with systemic risk due to having high impact capabilities must notify the European Commission. The European Commission can designate a GPAI model if it becomes aware of such a GPAI model presenting systemic risks of which it has not been notified. Moreover, the European Commission can proceed to a designation on the basis of specific criteria mentioned above. The scientific panel constituted under the AI Act can issue a qualified alert to the European Commission.
- Providers of GPAI models with systemic risk will be subject to additional obligations. These include: (i) performing model evaluation, in accordance with standardised protocols and tools reflecting the state of the art, including adversarial testing of the model to identify and mitigate systemic risks; (ii) assessing and mitigating possible systemic risks at Union level, including their sources; (iii) monitoring and reporting to relevant authorities on serious incidents and related corrective measures; and (iv)

<sup>10</sup> Directive (EU) 2019/790, article 4(3).

<sup>11</sup> Systemic risk means "a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the EU market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain".

ensuring adequate cybersecurity protection for the model and its physical infrastructure.

- A list of GPAI models with systemic risk will be published and kept up-to-date.

## **12. What are the specific transparency requirements for certain AI?**

Specific transparency requirements apply to specific AI systems or AI uses, e.g. AI systems interacting with people such as chatbots. Some apply to the provider, others to the deployer.

These provisions have been expanded to introduce new requirements including for generative AI, notably to ensure relevant content is identified or detectable as artificially generated or manipulated. Providers of AI systems, including GPAI systems, generating synthetic audio, image, video or text content will have to ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated. Likewise, deployers of an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest, like deployers of an AI system that generates or manipulates content constituting a deep fake, will have to disclose that the text / content has been artificially generated or manipulated.

There are also specific transparency requirements imposed on deployers to ensure people are aware where exposed to the operation of an emotion recognition or biometric categorisation system.

Exceptions and specificities may apply, e.g. law enforcement exceptions or, as regards deep fakes, in relation to artistic or satirical works.

## **13. What about the general core principles that were envisaged for all AI systems?**

The European Parliament had previously proposed to include requirements tied to a set of general ethical principles presented as applying to all AI systems. For more information on this, you can see our publication here for instance: [EU AI Act-Final negotiations can begin after Parliament vote](#).

These provisions have not been maintained as such. That said, they have not disappeared. The seven non-binding ethical principles from the 2019 Ethics Guidelines for Trustworthy AI, developed by the independent High-Level Expert Group on AI, continue to be recalled. According to the AI Act's recitals, those guidelines contribute to the design of trustworthy and human-centric AI. Further, the application of those principles should be translated, when possible, in the design and use of AI models, and they should in any event serve as a basis for the preparation of codes of conduct under the AI Act. Also, "[a]ll stakeholders, including industry, academia, civil society and standardisation organisations, are encouraged to take into account, as appropriate, the ethical principles for the development of voluntary best practices and standards".

In any event, the relevant ethical principles underlie many of the binding requirements that are contained in the AI Act, and they transpire throughout the text.

## Looking forward

### 14. How will the AI Act be enforced? What fines will apply?

(a) A strong enforcement and supervision framework is set up, at the national level and also at the EU level. Key bodies and authorities include national competent authorities, the AI Office established within the European Commission, the AI Board, the scientific panel of independent experts and the advisory forum provided under the AI Act.

The European Commission decision establishing the AI Office was published on 24 January 2024, in advance of the adoption of the AI Act, and it entered into force on 21 February 2024. On 29 May 2024, the European Commission unveiled the AI Office organisation and structure, with announced organisational changes said to take effect on 16 June 2024. On 19 June 2024, a first high-level meeting was also held by the European Commission with respect to the AI Board.

(b) There will be strong penalties including significant, gradual fines<sup>12</sup>:

<b>Prohibited practices</b>	up to the higher of EUR 35,000,000 and 7% of the undertaking's global annual turnover.
<b>High-risk AI and specific transparency requirements</b>	up to the higher of EUR 15,000,000 and 3% of the undertaking's global annual turnover.
<b>GPAI models<sup>13</sup></b>	up to the higher of EUR 15,000,000 and 3% of the provider's global annual turnover.
<b>Incorrect, incomplete or misleading information<sup>14</sup></b>	up to the higher of EUR 7,500,000 and 1% of the undertaking's global annual turnover.

Provision is made for the specific case of SMEs. For the latter, including start-ups, the fine will be up to the relevant percentage or amount, whichever is lower. This treatment does not seem to have been expressly extended to fines for providers of GPAI models, however. More generally, there are mechanisms aimed at adapting and simplifying rules under the AI Act for SMEs, including start-ups and micro-enterprises, e.g. as regards participation in regulatory sandboxes<sup>15</sup> – another key aspect of the AI Act.

In most cases, it is for the EU Member States to lay down the rules on penalties and other enforcement measures for infringements of the AI Act, in line with what the AI Act provides as well as guidelines that may be issued by the European Commission. On the other hand, and importantly, the European Commission has exclusive powers to supervise and enforce the provisions on GPAI models, including imposing fines on providers of such models – not the EU Member States.

In some instances, and whereas this was not the case initially, the fines are now set by reference to the turnover of the 'undertaking'. This could suggest that fines are intended to be calculated based on the turnover of the group, rather than just the individual entity responsible for the non-compliance. This change has not been explicated in the AI Act. If interpreted this way however, it could have very serious ramifications.

<sup>12</sup> Some requirements do not necessarily appear set to specific fines.

<sup>13</sup> For infringements by providers of GPAI models of their obligations, or in case they fail to comply with a request for documents or information, supply incorrect, incomplete, or misleading information or fail to comply with other relevant requests or enforcement measures.

<sup>14</sup> For the supply of incorrect, incomplete, or misleading information to competent authorities or notified bodies in reply to a request, subject to the specific rules above for GPAI models.

<sup>15</sup> Various measures have also been launched in parallel to support European SMEs and start-ups, including as regards access to AI super-computing infrastructure and capacity for the training of models.

## 15. What secondary legislation and guidance are we expecting going forward?

The AI Act is a complex and technical piece of legislation, and it is to be supplemented by secondary legislation, guidelines and other supporting documentation, with a limited number having been set to specific timelines.

Examples of documents to be adopted under the AI Act include:

- (a) **Delegated and implementing acts:** The European Commission will for instance adopt implementing acts to: (i) detail arrangements and procedural safeguards for proceedings aimed at imposing fines with respect to GPAI models; (ii) specify the detailed arrangements / elements for regulatory sandboxes and the real-world testing plan; and (iii) establish a template for the post-market monitoring plan and the list of elements it must include. The implementing act for item (iii) is to be adopted by 2 February 2026. Through delegated acts, it will also for instance amend the filter system to remove conditions where there is evidence that this is necessary to maintain the level of protection provided for by the AI Act. Likewise, the European Commission will adopt delegated acts to amend the thresholds for the classification of GPAI models as GPAI models with systemic risk, including the presumption, as well as to supplement benchmarks and indicators in light of evolving technological developments, for the thresholds to reflect the state of the art.
- (b) **Guidelines:** The European Commission will develop various guidelines, in particular on the practical implementation of the AI Act. For instance, by no later than 2 February 2026, the European Commission must provide guidelines on the practical implementation of the filter system, completed by a comprehensive list of practical examples of use cases of AI systems that are high-risk and use cases that are not high-risk AI systems. Other examples include guidelines on (i) the prohibited practices, (ii) the application of the definition of an AI system, (iii) the application of the requirements, and responsibilities along the AI value chain, for high-risk AI systems, (iv) the practical implementation of the specific transparency obligations, as well as (v) detailed information on the relationship between the AI Act and other EU legislation as mentioned above. Whilst they are not set to express timeframes in the AI Act, the AI Office is said to be preparing the guidelines on the AI system definition and on the prohibitions, due six months after entry into force of the AI Act.
- (c) **Codes of practice, codes of conduct, templates, harmonised standards:** Providers of GPAI models will be able to rely on codes of practice to demonstrate compliance with applicable requirements, until a harmonised standard is published. Accordingly, and to enable providers to demonstrate compliance on time, codes of practice are to be ready at the latest 9 months after the entry into force of the AI Act (i.e., by 2 May 2025), with the AI Office having to take the necessary steps to that effect. There are specific mechanisms in case codes of practice cannot be finalised within a given timeframe, however. The AI Office is also tasked with developing such things as a template for (i) a questionnaire to facilitate deployers' compliance with their obligations regarding the FRIA, as well as (ii) the summary to be made available by providers of GPAI models regarding the content used to train the model. Important developments are also expected in terms of standardisation.

Also, in various other circumstances, the European Commission will be entitled to adopt further documentation, including secondary legislation or voluntary model terms for contracts between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used for or integrated into high-risk AI systems.

\*\*\*\*\*

The AI Act will clearly change how businesses approach AI, and what they need to consider and do when looking to develop, have developed, supply, put on the market or into service, use, brand, modify, import or distribute AI systems or AI models, or other items used in AI systems.

Organisations will need to ask themselves a number of key questions, to carry out necessary assessments, to implement appropriate frameworks, measures, systems, processes and policies to comply with their obligations, to upskill staff, to monitor developments including potential incidents, etc.

Many businesses have already started planning, preparing and possibly also adapting in anticipation of the AI Act. It is time to really ramp up efforts, with the EU's new AI rulebook now becoming a reality.

After years spent shaping these new rules, the attention will now turn to the effective implementation and enforcement of the AI Act. In parallel, other rules continue to be developed and adopted, in the EU and beyond.

# CLIFFORD CHANCE

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

[www.cliffordchance.com](http://www.cliffordchance.com)

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2024

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to [nomorecontact@cliffordchance.com](mailto:nomorecontact@cliffordchance.com) or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.