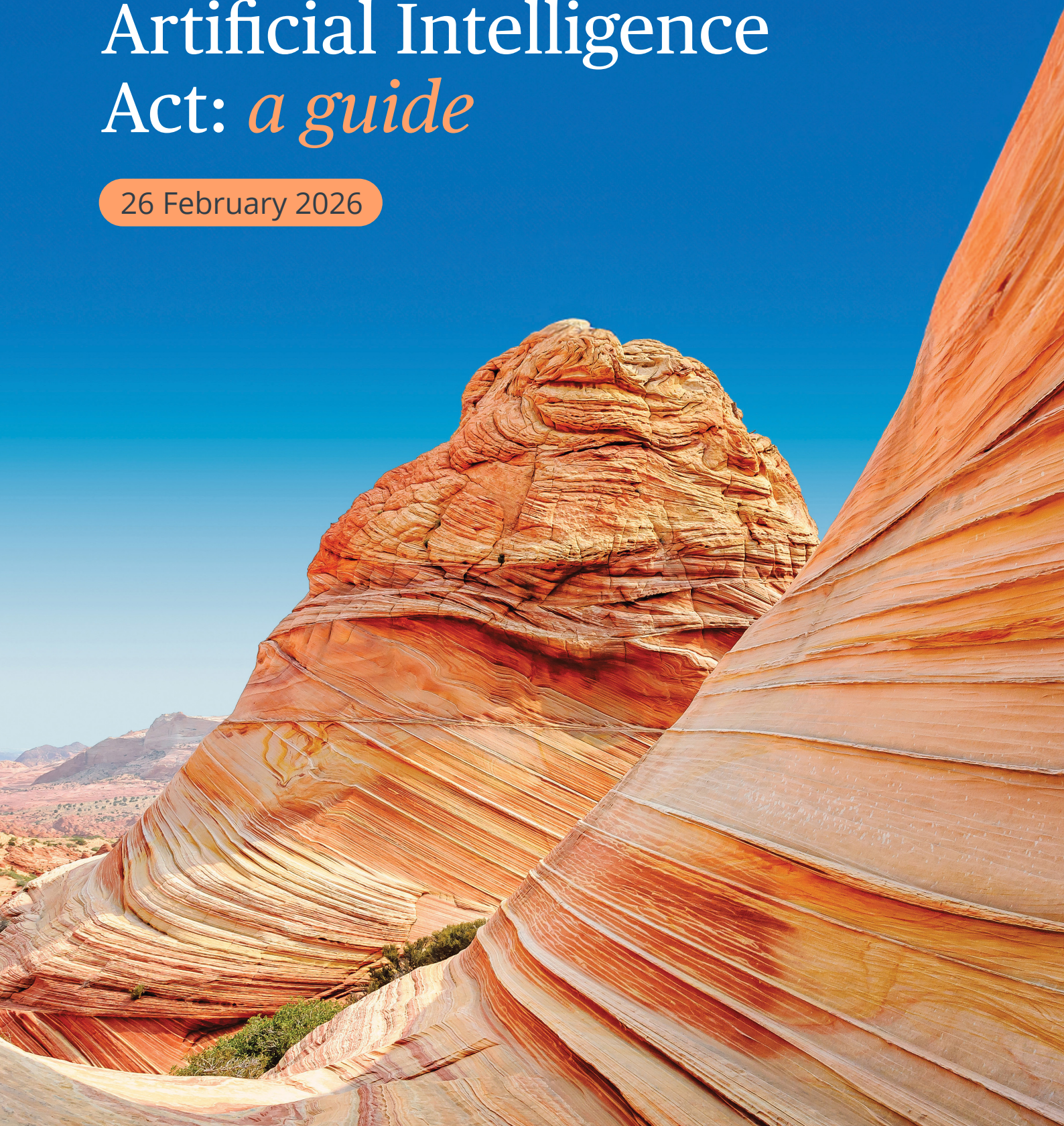
Bird & Bird

European Union Artificial Intelligence Act: *a guide*

26 February 2026



Contents

1 OVERVIEW, KEY CONCEPTS & TIMING OF IMPLEMENTATION

Overview
Key concepts
Timeline

2 MATERIAL AND TERRITORIAL SCOPE

Material scope
Territorial scope
Exclusions
Relationship with other regulatory frameworks

3 PROHIBITED AI PRACTICES

Prohibited AI practices
To whom do the prohibitions apply?
Enforcement and Fines

4 HIGH-RISK AI SYSTEMS

Classification of an AI system as a high-risk AI system
Obligations for providers of high-risk AI systems
Harmonised standards and conformity assessment procedure for providers of high-risk AI systems
Obligations for deployers of high-risk AI systems
Obligations for other parties in connection with high-risk AI systems

5 GENERAL-PURPOSE AI MODELS

Background and relevance of general-purpose AI models of personal data
Terminology and general-purpose AI value chain
Obligations for providers of general-purpose AI models
General-purpose AI models with systemic risk

6 TRANSPARENCY OBLIGATIONS

General transparency obligations
Transparency obligations for high-risk AI systems
Transparency obligations at the national level and codes of practice
Relationship with other regulatory frameworks

7 REGULATORY SANDBOXES

AI regulatory sandboxes
Real-world testing of AI systems

8 ENFORCEMENT & GOVERNANCE

Overview
Post-marking obligations
Market surveillance authorities
Procedures for enforcement
Authorities protecting fundamental rights
General-purpose AI models
Penalties
Remedies for third parties
Governance

9 AI ACT: WHAT'S NEXT

AI Act: What's Next
Delegated Acts
Implementing Acts
Commission Guidelines
Codes of conduct and practice
Standards

10 OUR GLOBAL CONTRIBUTORS

Overview, key concepts & timing of implementation

Overview

The European Union (EU) stands as a pioneer in the regulation of artificial intelligence (AI), setting a global benchmark with its proactive approach to ensuring ethical and responsible AI development. Indeed, it seems we may witness a new Brussels effect, reminiscent of the influence wielded by the GDPR. The EU's comprehensive and precautionary framework prioritises transparency, accountability, and human rights.

The AI Act applies beyond the borders of the EU – many of its provisions apply regardless of whether the providers are established or located within the EU or in a third country. The AI Act applies to any provider or entity responsible for deploying an AI system if "the output produced by the system is intended to be used" in the EU. Foreign suppliers must appoint an authorised representative in the EU to ensure compliance with the AI Act's provisions. However, the AI Act does not apply to public authorities of third countries or to international organisations under police and judicial cooperation agreements with the EU, nor to AI systems placed on the market for military defence or national security purposes. This broad scope aims to ensure comprehensive regulation of AI systems and their uses.

While pioneering, the AI Act adds significant complexity for many organisations which provide and deploy AI system in the EU. Critics have highlighted that some obligations under the AI Act are difficult and costly to implement in practice, with complex obligations, unclear timing for key supporting elements such as harmonised standards, and administrative burdens that risk hindering European innovation and competitiveness.

In November 2025, the Commission published a proposal for a Digital Omnibus Regulation, which includes targeted technical amendments to certain elements of the AI Act. These amendments are aimed at lowering compliance costs, ensuring smoother and more proportionate implementation, and stimulating competitiveness without undermining the AI Act's core objectives.

At the time of writing, the Digital Omnibus Regulation remains in draft form and will need to pass through the EU's legislative process before any amendments to the AI Act will come into effect.

What you can expect from this guide

- This chapter provides an overview of the whole AI Act, its key concepts and the dates from when its provisions will apply.
- Chapter 2 looks at the territorial and material scope of the AI Act.
- Chapters 3, 4, 5 and 6 address the requirements which the AI Act imposes on different types of AI – prohibited AI practices; high-risk AI systems; general purpose AI models; and AI systems subject to specific transparency obligations.
- Chapter 7 explains the AI Act's arrangements for testing AI in regulatory sandboxes. Chapter 8 looks at governance and enforcement.
- Chapter 9 summarises the numerous further measures that have to follow the adoption of the AI Act.
- Chapter 10 includes all the contributors to this guide.
- Proposed changes to the AI Act under the draft Digital Omnibus Regulation are highlighted in the relevant Chapters and summarised together in Chapter 9.

A risk-focused approach

The EU approach to AI regulation is characterised by its risk-based framework. This regulation adopts a technology-neutral perspective, categorising AI systems based on their risk level, ranging from minimal to high-risk. This approach

ensures that higher-risk AI applications, particularly those that can significantly impact fundamental rights, are either prohibited or subjected to stricter requirements and oversight.

The EU places a strong emphasis on promoting the development and use of responsible AI. The AI Act mandates strict measures for data security and user privacy, ensuring that AI systems are designed and deployed with these considerations at the forefront. This includes rigorous requirements for how data is handled and protected, ensuring that users' personal information remains secure.

Additionally, the AI Act requires comprehensive risk assessments for AI systems considered to be high-risk. These assessments help identify and mitigate potential risks associated with AI technologies, fostering transparency and accountability among AI providers. By making these evaluations mandatory, the EU ensures that AI developers thoroughly understand and address the implications of their technologies.

This proactive approach aims to build public trust in AI technologies by protecting users' rights and well-being. By prioritising data security, privacy, and risk management, the EU seeks to reassure the public that AI can be used safely and ethically. This focus on responsible development helps to promote broader acceptance and integration of AI technologies, ultimately benefiting society as a whole. The AI Act has been developed not only to create laws for AI systems, but also to establish an ethical framework for their use, to ensure that organisations consider the impact of their AI systems on people, other businesses, the environment and many other aspects of our lives.

Ethics is embedded in the AI Act

The AI Act explicitly builds on the Ethical Guidelines on Trustworthy AI, which were published by the Commission in 2019. While these guidelines remain non-binding, many of their principles have been directly incorporated into the AI Act. This is best demonstrated by the many provisions of the AI Act, that directly refer to the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union. For example, high-risk AI systems are those that have a significant harmful impact on the health, safety and fundamental rights of persons in the EU.

The proper application of the AI Act will therefore in many cases require an analysis of the risks to fundamental rights, which includes both legal and ethical issues.

Governance

The EU adopts a decentralised supervision model, promoting collaboration with various national authorities. The AI Act establishes the European Artificial Intelligence Office (AI Office) as an independent entity, serving as the central authority on AI expertise across the EU, and playing a crucial role in implementing the legal framework. The AI Office encourages the development of trustworthy AI and supports international collaboration. It also serves as the secretariat of the European Artificial Intelligence Board (AI Board), which is composed of one representative from each EU Member State, with the European Data Protection Supervisor participating as an observer. The AI Board plays a key role in the governance framework established by the AI Act.

The AI Office aims to promote and facilitate the creation, review, and adaptation of codes of good practice, considering international approaches. To ensure these codes reflect the current state of the art and incorporate diverse perspectives, the AI Office will collaborate with relevant national authorities and may consult with civil society organisations, stakeholders, and experts, including scientific experts.

Key concepts

AI systems (see also Chapter 2)

> Most of the AI Act applies to *"AI systems"*, which the Act defines as "*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*".

The AI Act does not define "artificial intelligence", but it does define the term "artificial intelligence system". The definition of an AI system is intentionally consistent with the OECD definition of an AI system. The definition does not mention any specific technology or currently known approaches to artificial intelligence systems. With the rapidly evolving nature of AI, this prevents the AI Act from becoming obsolete due to technological developments.

A key element of this definition is the AI system's ability to "infer". This is intended to allow for a clear distinction between AI systems and traditional software. If a computer program operates according to rules defined in advance by the programmers, it is not an AI system; if a system is built using techniques that allow the program to create rules of its own based on input data or data sets provided to the program, then it is an AI system. The definition of an AI system is discussed further in guidelines published by the Commission on 6 February 2025.

Obligations across the supply chain
(see also Chapter 2)

The AI Act potentially applies to all participants in the supply chain, starting with the "provider", who carries primary responsibility for most obligations under the Act. The scope also includes the 'deployer' 'importer' and 'distributor', each of whom is subject to their own obligations relating to the handling or use of an AI system. While the provider holds the core responsibilities, importers and distributors situated between the provider and the deployer must ensure that the AI systems they import or distribute comply with the requirements of the AI Act.

An importer, distributor or deployer may themselves become a provider of a high-risk AI system if they put their name or trademark on a high-risk AI system. They may also become a provider of a high-risk system if they make substantial modifications to, or modify the intended purpose of the AI system, which renders the system high-risk.

Risk approach to classification of AI systems

A risk-based classification of AI systems is a fundamental aspect of the AI Act, focusing on the potential harm to health, safety, and fundamental human rights that an AI system may cause. This approach categorises AI systems into three distinct risk levels with specific rules applying to each level:

1. **Unacceptable risk:** AI systems that pose such significant risks are unacceptable and therefore prohibited.

2. **High-risk:** High-risk AI systems are subject to stringent regulatory requirements.

3. **Minimal or no risk:** AI systems that pose minimal or no risk have no regulatory restrictions under the AI Act.

In addition to the general risk classification of AI systems, the AI Act also imposes specific **transparency obligations** on certain AI systems. For systems classified as high-risk, these transparency obligations will apply in addition to the requirements already established for high-risk systems.

Unacceptable risk: prohibited practices
(see also Chapter 3)

The AI Act contains a list of prohibited AI practices, which in the EU, prohibit placing on the market, putting into service, or using an AI system that employs any of these practices. The list prohibits:

- using subliminal techniques or purposefully manipulative or deceptive techniques to materially distort behaviour, leading to significant harm;

- exploiting vulnerabilities of an individual or group due to their specific characteristics, leading to significant harm;

- social scoring systems i.e. evaluating or classifying of an individual or group based on their social behaviour or personal characteristics, leading to detrimental or unfavourable treatment;

- evaluating a person's likelihood of committing a criminal offence, based solely on profiling or personal characteristics; except when used to support human assessment based on objective and verifiable facts linked to a criminal activity;

- facial recognition databases based on untargeted scraping from the internet or CCTV;

- inferring emotions in workplaces or educational institutions, except for medical or safety reasons;

- biometric categorisation systems that categorise a person based on their sensitive data, except for labelling or filtering lawfully acquired biometric datasets such as images in the area of law enforcement;

- real-time remote biometric identification systems in publicly available spaces for law enforcement purposes, except in narrowly defined circumstances.

In some cases, the AI Act contains exceptions that allow these "prohibited" practices to be used in certain situations. For example, real-time biometric identification in public places for law enforcement purposes is allowed by the Regulation only in limited circumstances and is subject to prior authorisation. The Commission published guidelines on the scope and application of the prohibited AI practices rules on 4 February 2025.

High-risk AI systems (see also Chapter 4)

The extensive regulation of high-risk AI systems constitutes a major part of the AI Act. AI systems are identified as high-risk AI systems if they have a significant harmful impact on the health, safety and fundamental rights of persons in the EU. There are two categories of high-risk AI systems which are regulated differently:

- AI systems intended to be used as a product or a safety component of a product which is covered by EU harmonisation legislation, such as civil aviation, vehicle security, marine equipment, radio equipment, toys, lifts, pressure equipment, medical devices, personal protective equipment (listed in Annex I to the AI Act).

- AI systems listed in Annex III of the AI Act, such as AI used in education, employment, credit scoring, law enforcement, migration, remote biometric identification systems, and AI systems used as a safety component in critical infrastructure. This list can be amended by the Commission.

The first category of high-risk systems is covered by both the harmonisation legislation and the AI Act. Providers have an option of integrating the requirements of the AI Act into the procedures required under the respective EU harmonisation legislation listed in Section A of Annex I. In addition, only selected provisions of the AI Act apply to high-risk AI systems in relation to products covered by EU harmonisation legislation listed in Section B of Annex I (such as aviation equipment).

The Commission was due to provide guidance on the classification of high-risk AI systems by 2 February 2026. Once published, this should include a comprehensive list of practical examples of use cases of high-risk and non-high-risk AI systems.

Exceptions to the qualification of high-risk AI system

If a high-risk AI system listed in Annex III 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, it will not be treated as a high-risk AI system.

Such situations may only arise in four cases where the AI system is intended to:

- perform a narrow procedural task;

- improve the result of a previously completed human activity;

- detect decision-making patterns or deviations from prior decision-making patterns, and is not meant to replace or influence the previously completed human assessment without proper human review; or

- perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.

If, however, the AI system performs profiling of natural persons, it is always considered a high-risk AI system and cannot fall into one of the above exceptions.

Although the AI Act's rules for high-risk AI systems have not yet become applicable, there are strong indications that this exemption will play an important role in practice, as it allows organisations to avoid the obligations and costs associated with placing a high-risk AI system on the market. One option is, for example, to carve out those parts of an AI system that can take advantage of this exemption to limit the scope of the high-risk AI system.

However, even if a provider relies on the exemption, its assessment of the AI system must be documented, and the AI system must still be registered in the EU database for high-risk AI systems before it is placed on the market or put into service. The draft Digital Omnibus Regulation proposes removing the registration obligation, while retaining the requirement for the provider to document why it considers the AI system to fall within the exception.

Extensive requirements for high-risk AI systems

The requirements that must be met by providers of high-risk AI systems are strict. These requirements include, in particular, the need to document every stage of the development of the AI system, to meet obligations regarding the use of high-quality data for training, to produce system documentation that provides users with full information about the nature and purpose of the system, and to ensure the accuracy, robustness and cybersecurity of the systems. High-risk AI systems will also have to be registered in an EU database, which will be publicly available.

Obligations across the supply chain of high-risk AI systems

The AI Act imposes obligations on all participants in the supply chain of a high-risk system throughout its life cycle. The responsibilities are not only those of the 'provider', but also those of any 'importer', 'distributor' and 'deployer' of the AI system, although most of the responsibilities lie with the provider and the deployer.

The primary duty of the importer and distributor is to verify that the high-risk AI system being imported or distributed meets the requirements of the AI Act. Moreover, an importer, distributor or deployer may become a provider of the high-risk AI system if they have put their name or trademark on the AI system, made substantial modifications or they have modified the intended purpose of the AI system, which renders the system high-risk.

General-purpose AI models (see also Chapter 5)

The distinction between AI models and AI systems is crucial for the application of the AI Act. AI models are essential components of AI systems, but they do not constitute AI systems on their own. AI models require the addition of other components, such as a user interface, to become AI systems. The AI Act mostly regulates AI systems, not models. However, it *does* contain rules on general-purpose AI models.

The AI Act provides rules for all general-purpose AI models and additional rules for general-purpose AI models that pose systemic risks. These rules apply in the following situations:

- where the provider of a general-purpose AI model integrates its own model into its own AI system that is made available on the market or put into service;
- where the provider of a general-purpose AI model only offers its own model to providers of AI systems.

The Commission published Guidelines on the scope of obligations for providers of general-purpose AI models under the AI Act on 18 July 2025. It also published a Code of Practice that providers of general-purpose AI models can use as a voluntary tool to demonstrate compliance with the general-purpose AI model rules under the AI Act. The Code of Practice consists of three chapters; *Transparency and Copyright* which apply to all general-purpose AI models and a *Safety and Security* chapter which applies to general-purpose AI models with systemic risk.

Transparency obligations (see also Chapter 6)

The AI Act includes transparency obligations for four types of AI systems (which may or may not also be classified as a high-risk system):

- AI systems designed to interact directly with natural persons;
- AI systems, including general-purpose AI systems, that generate synthetic audio, image, video or text content;
- emotion recognition or biometric categorisation systems;
- AI systems that generate or manipulate images, audio or video that are deepfakes.

In all these cases, the user must be informed about the use of the AI system. There are also more detailed obligations, for example to mark the output in a machine-readable way so that it can be identified as artificially generated or manipulated. Guidelines on the scope and application of transparency obligations are under development by the Commission at the time of writing, along with a Code of Practice relating to synthetic audio, image, video or text content and deepfakes.

Complex supervision and enforcement structure (see also Chapter 8)

The AI Act provides for a complex, multi-level structure for overseeing implementation, covering both national and EU level entities. At each level there will be several types of bodies, such as notifying authorities and notified bodies, conformity assessment bodies, the AI Board, the AI Office, national competent authorities and market surveillance authorities.

These authorities will not only control compliance, but also support the market by, among other things, developing codes of conduct, organising AI regulatory sandboxes (see also Chapter 7) and providing support for SMEs and start-ups.

Role of technical standards, Codes of Practice and guidelines (see also Chapters 7, 8 and 9)

The AI Act can be seen as a framework for more detailed obligations that will result from various further documents and legal acts. Most notably, we can expect that technical standards will play very important role in the practical application of the AI Act.

The AI Act requires providers of high-risk AI systems to affix a European Conformity (CE) marking. The CE marking will show compliance with the requirements of the AI Act. For the mark to be affixed, providers will have to apply harmonised technical standards or otherwise be able to demonstrate how they are complying with the requirements of the AI Act. In addition, high-risk AI systems or general-purpose AI models which are in conformity with harmonised standards shall be presumed to be in conformity with the requirements of the AI Act to the extent that those standards cover those requirements or obligations. Consequently, the general provisions of the AI Act will be complemented by detailed technical standards that will provide concrete methods for demonstrating compliance with the AI Act.

Codes of Practice also play an important role in setting out more detailed compliance requirements. The AI Office can encourage and facilitate the development of Codes of Practice and the Commission can then, by way of an implementing act, approve a Code of Practice and give it a general validity within the EU. This process has already been followed for general-purpose AI model rules, with the resulting Code of Practice having been published in July 2025 and approved by the Commission on 1 August 2025. A Code of Practice for specific transparency obligations is under development and is expected to be finalised during 2026. In addition to Codes of Practice, the Commission has the obligation to develop several guidelines on the practical implementation of the AI Act.

Enforcement (see also Chapter 8)

The AI Act provides for significant administrative fines for non-compliance, with the applicable penalty depending on the infringement and, for undertakings, their worldwide annual turnover. The Act establishes a tiered system of fines to ensure proportionality while reserving the highest penalties for the most serious violations.

In particular:

- Non-compliance with the prohibitions on certain AI practices set out in article 5 may result in administrative fines of up to €35 million or, in the case of an undertaking, up to 7% of total worldwide annual turnover, whichever is higher.
- Infringements of other obligations under the AI Act, including those relating to high-risk AI systems and general-purpose AI models, may be sanctioned with administrative fines of up to €15 million or, for undertakings, up to 3% of total worldwide annual turnover, whichever is higher.
- The supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request or may be subject to administrative fines of up to €7.5 million or, for undertakings, up to 1% of total worldwide annual turnover, whichever is higher.

These penalties underscore the importance of complying with the AI Act's regulations. It is essential for companies to fully grasp these penalties and ensure that their AI systems and general-purpose AI models meet the Act's requirements.

Timeline

The AI Act is becoming applicable on a staggered basis. There are also transitional arrangements for AI systems that had been placed on the market or put into service before certain dates.

The relevant dates of application are set out below.

12 July 2024	The AI Act was published in the Official Journal of the EU, triggering the dates for specific provisions in the Regulation becoming applicable.
2 February 2025	Prohibited practices ban applies (Chapter II). AI literacy rules apply (article 4).
2 August 2025	National authorities designated (Chapter III Section 4). Obligations apply for general-purpose AI models placed on the market on or after this date (Chapter V). Governance (at EU and national level) (Chapter VII). Confidentiality and penalties (other than in relation to general-purpose AI models) (Chapter XII).
2 August 2026	Start of application of all other provisions of the EU AI Act (unless a later date applies below), e.g. article 50 transparency obligations and obligations for operators of high-risk AI systems listed in Annex III which are placed on the market or put into service (or substantially modified) after this date.
2 August 2027	Obligations apply for operators of high-risk AI systems listed in Annex I which have been placed on the market or put into service (or substantially modified) on or after 2 August 2026. Obligations apply for general purpose AI models placed on the market before 2 August 2025 (article 111).
2 August 2030	Obligations apply for providers and deployers of high-risk AI systems (other than those listed below), which have been placed on the market or put into service before 2 August 2026 and which are intended to be used by public authorities (article 111).
31 December 2030	Obligations apply for components of large-scale IT systems listed in Annex X, which have been placed on the market or put into service before 2 August 2027 (article 111).

To reflect the time it has taken to prepare key supporting elements, such as harmonised standards for high-risk systems, the draft Digital Omnibus Regulation proposes extending the deadlines for high-risk AI systems as follows:

- **High-risk AI systems listed in Annex III:** The current deadline of 2 August 2026 would be extended to the earlier of (i) six months after publication of a decision of the Commission confirming that adequate measures (i.e. harmonised standards, common specifications, Commission guidelines) in support of compliance with Chapter III are available; or (ii) 2 December 2027.
- **High-risk AI systems listed in Annex I:** The current deadline of 2 August 2027 would be extended to the earlier of (i) twelve months after publication of a decision of the Commission confirming that adequate measures in support of compliance with Chapter III are available; or (ii) 2 August 2028.

Material and territorial scope

At a glance

- The AI Act covers AI systems, general-purpose AI models and prohibited AI practices.
- Obligations can be imposed on six categories of economic actors: providers, importers, distributors, product manufacturers, authorised representatives and deployers.
- Economic operators involved with high-risk AI systems have significant obligations. Providers and deployers of certain categories of AI systems are also subject to transparency obligations.
- Providers of general-purpose AI models are subject to obligations.
- The AI Act applies when an AI system or general-purpose AI model is placed on the EU market, put into service in the EU, imported into or distributed in the EU. It also applies where an AI system is used by a deployer who has their place of establishment or is in the EU.
- Providers and deployers of AI systems who fall within scope of the AI Act have become subject to AI literacy requirements from 2 February 2025 (although it should be noted that the draft Digital Omnibus Regulation proposes removing the literacy obligations for providers and deployers).

To do list

- [ ] Determine whether you, your suppliers or your customers will be an operator falling within the material and territorial scope of the AI Act.
- [ ] If you or your supply or distribution chain fall within the scope of the AI Act, check whether any AI systems or AI models fall within one or more of the regulated categories.
- [ ] If you are a provider or deployer of AI systems within the scope of the AI Act, ensure you are complying with the Act's AI literacy requirements.

Material scope

The AI Act primarily provides harmonised rules for the placing on the market, the putting into service, and the use of AI systems. It imposes an extensive set of obligations on *"high-risk"* AI systems and transparency obligations on certain AI systems. It also prohibits certain AI practices and regulates the supply of general-purpose AI models in the EU.

The AI Act also sets out rules for market monitoring, market surveillance, governance and enforcement, which includes administrative fines, as well as measures to support innovation, with a particular focus on small and medium enterprises, such as through the operation of AI sandboxes. It also establishes two new bodies: (i) the European Artificial Intelligence Board (the board) – which is tasked with advising and assisting the Commission and EU Member States to facilitate the consistent and effective application of the AI Act; and (ii) the AI Office, which has been established within the Commission and is tasked with implementing the AI Act, fostering the development and use of trustworthy AI and promoting international cooperation.

Regulated persons: Operators

The AI Act imposes obligations on six categories of operators: providers, deployers, importers, distributors, product manufacturers and authorised representatives. The term *"operator"* is used to describe all of them. There will always be a provider for an AI system or a general-purpose AI model. Whether there will also be other operators will depend on the way in which the AI system or general-purpose AI model is being supplied and deployed. Most operators are defined with reference to three key terms adapted from the EU product legislation referenced in Annex I: *"making available"*, *"placing on the market"* and *"putting into service"*.

"making available" is the supply of an AI system or a general-purpose AI model for distribution or use on the EU market in the course of a commercial activity, whether in return for payment or free of charge;

"placing on the market" is the first making available of an AI system or a general-purpose AI model on the EU market; and

"putting into service" is the supply of an AI system for first use directly to the deployer or for own use in the EU for its intended purposes.

The term *"use"* is not defined in the AI Act. In essence, *"use"* would be perceived by reference to the key characteristic of an AI system which is to infer, from inputs it receives, how to generate outputs. These three terms *"making available", "placing on the market" and "putting into service"* are discussed in section 2.3 of the Commission's Guidelines on prohibited AI practices, which provides illustrative examples of each activity in the context of the restrictions on prohibited practices.

The regulated operators under the AI Act are:

Operator		Role
Relevant for both AI systems and general-purpose AI models	**Provider (article 3(3))**	Develops an AI system or a general-purpose AI model or has an AI system or a general-purpose AI model developed *and* places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge. Although the definition of *"placing on the market"* refers to the EU market, a person can still be deemed a provider regulated by the AI Act even if they do not place an AI system on the EU market, where the output of the AI system is used in the EU. See *"Territorial Scope"* further below. A provider can be a natural or legal person, public authority, agency or other body. EU institutions, bodies, offices and agencies may also act as a provider of an AI system.

		It is also possible to become a provider where a high-risk AI system has already been placed on the market or put into service in the EU by another provider, by taking one of the steps set out in article 25(1)(a)-(c). See further below, under *"High-risk AI systems"*.
	Authorised representative (article 3(5))	An EU-established natural or legal person appointed by a provider of a high-risk AI system or general-purpose AI model established outside the EU to act as their authorised representative. The role includes ensuring that the documentation required by the AI Act is available to the competent authorities and co-operating with those authorities. See article 22 (for high-risk AI systems) and article 54 (for general-purpose AI models).
Relevant for AI systems only	**Deployer (article 3(4))**	Uses an AI system under its authority (excluding use in the course of personal, non-professional activity). A deployer can be a natural or legal person, public authority, agency or other body. EU institutions, bodies, offices and agencies may also act as a deployer of an AI system.
	Importer (article 3(6))	Natural or legal person located or established in the EU that places an AI system bearing the name or trademark of a person not established in the EU on the EU market.
	Distributor (article 3(7))	Natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market.
	Product manufacturer (article 25(3))	In certain circumstances, a product manufacturer will be considered the *"provider"* of a high-risk AI system where: this is a safety component of a product covered by the AI Act (by virtue of being subject to the EU product safety legislation referenced in Section A of Annex I), and the manufacturer places the AI system on the EU market or puts it into service in the EU together with that product and under its own name or trademark. The term *"product manufacturer"* is not defined in the AI Act but Recital 87 clarifies that this is the *"manufacturer"* defined under the EU product safety legislation referenced in Annex I to the AI Act.

Indirect obligations under the AI Act

The AI Act imposes indirect obligations on component suppliers to providers of high-risk AI systems. Those supplying AI systems, tools, services, components, or processes that are used or integrated in a high-risk AI system are required to enter into a written agreement with the provider of the high-risk AI system and to enable the latter to comply with its obligations under the AI Act (article 25(4)). This obligation does not apply to third parties who make such tools, services, processes or components (other than general-purpose AI models) accessible to the public under a free and open-source licence.

Rights granted by the AI Act

The AI Act confers a right to explanation of individual decision-making on affected persons located in the EU (article 86). Affected persons are those who are subject to a decision which has a legal or similarly significant effect on them and which is based on the output of one of the high-risk AI systems identified in Annex III. The wording used here is similar to that used under the automated decision-making provisions of the GDPR (article 22 GDPR); the scope of the two provisions however is not identical.

Regulated subject matter: AI systems

> An AI system is defined broadly in article 3(1) as: "*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*".

This definition is intended to align with the definition used by the OECD AI Principles. A key characteristic of AI systems is their capability to infer, i.e. to obtain outputs and to derive models or algorithms, or both, from inputs or data. In turn, traditional software, which executes operations based solely on rules defined by natural persons is not, on its own, considered an AI system.

In February 2025, the Commission published guidelines for this definition. These guidelines provide further explanations for each aspect of the definition, with a clear emphasis on the "ability to infer." In a positive sense, the guidelines outline various machine learning approaches that enable this ability. At the same time, they list systems – particularly those primarily based on mathematical or statistical methods – that do not possess this ability and should therefore not fall within the scope of the AI Act. A noteworthy example of systems that do not possess the ability to infer is "*logistic regression,*" which is widely used in the financial sector.

An AI system can be used on a standalone basis or as a component of a product, irrespective of whether the AI system is physically integrated into the product or serves the product's functionality without being integrated into it.

Under the AI Act, AI systems fall into one of the following categories:

- high-risk AI systems;
- all other AI systems.

Certain AI systems in either category can also be subject to specific transparency obligations. An AI system can also form part of a prohibited AI practice. This can be because of certain features of that AI system or because of the way the AI system would be used.

High-risk AI systems

Section III regulates high-risk AI systems. These are AI systems that pose a significant risk of harm to the health, safety and fundamental rights of persons in the EU. An AI system may be classified as high-risk in two ways:

- Article 6(1): The AI system is used as a safety component in a product that is regulated by certain EU product safety legislation (the EU harmonisation legislation listed in Annex I) and is subject to the conformity assessment procedure with a third-party conformity assessment body under such legislation, or constitutes on its own such a product (e.g. an AI system which is used for medical diagnostic purposes will itself be a regulated medical device); or
- Article 6(2): The AI system falls within one of the eight categories set out in Annex III – unless the provider can demonstrate and document that such AI system does not pose a significant risk of harm.

Most of the obligations regarding high-risk AI systems fall on providers (which includes product manufacturers as we describe further above), whilst a more limited set of obligations is imposed on deployers, on importers and distributors, and where relevant, authorised representatives.

See Chapter 4 of this guide for more details.

AI systems subject to transparency obligations

The AI Act imposes certain transparency obligations on:

- providers of AI systems intended to interact directly with natural persons (article 50(1));
- providers of AI systems generating synthetic audio, image, video or text content (article 50(2));
- deployers of an emotion recognition system or a biometric categorisation system (article 50(3)); and

- deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake (article 50(4)).

See Chapter 6 of this guide for more details.

All other AI systems

All other types of AI systems, which do not fall under the above categories and are not used for prohibited AI practices are not subject to direct legal obligations under the AI Act. Voluntary codes of conduct may be drawn up in future covering this broader category of AI systems and those deploying them (article 95). Providers and deployers may choose to adhere to these codes of conduct.

Aside from rules relating to specific categories of AI systems, those qualifying as the provider or deployer of any AI system under the AI Act are required to take AI literacy measures to ensure that their staff and other persons dealing with the operation and use of AI systems on their behalf, have a sufficient level of knowledge, skills and understanding regarding the deployment of AI systems, their opportunities and risks (article 4). This obligation aims to foster the development, operation and use of AI in a trustworthy manner in the EU. The AI Act does not provide for a specific stand-alone administrative fine for breach of the AI literacy in article 4. However, enforcement is left to national market surveillance authorities, which may establish penalties under national law. A failure to ensure appropriate AI literacy could also be considered as an aggravating factor when authorities assess compliance with other obligations under the AI Act.

The draft Digital Omnibus Regulation proposes removing the AI literacy obligation imposed on providers and deployers by article 4 and replacing it with a general responsibility for the Commission and EU Member States to promote AI literacy. This proposal remains subject to negotiation and adoption, during which time article 4 remains in force.

Regulated subject matter: Prohibited AI practices

The AI Act prohibits the placing on the market, putting into service and use of AI systems that have certain prohibited features and/or are intended to be used for certain prohibited purposes, e.g. AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage. These practices are deemed to be particularly harmful and abusive and contradict EU values and fundamental rights. The prohibited AI practices are listed in article 5. This list does not affect the prohibitions of AI practices that infringe other EU law (such as data protection, non-discrimination, consumer protection and competition law).

See Chapter 3 of this guide for more detail.

Regulated subject matter: general-purpose AI models

A general-purpose AI model is defined in article 3(63) 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*".

The AI Act does not provide a definition of an "*AI model*". Recital 97 notes that although AI models are essential components of AI systems, they do not constitute AI systems on their own and require further components, such as a user interface, to become AI systems. The characteristics of general-purpose AI models are discussed further in recitals 98 and 99.

Where can I find this?

Material Scope article 1 recitals 1-3, 6-8

The AI Act regulates general-purpose AI models and imposes additional obligations for general-purpose AI models with systemic risks. The rules apply to providers of general-purpose AI models, once these models are placed on the market. This can be done in various ways, such as through libraries, APIs, as a direct download or as a physical copy.

Recital 97 suggests that the rules on general-purpose AI models can also apply when these models are integrated into or form part of an AI system. When the provider of a general-purpose AI model integrates its own model into its own AI system that is made available in the market or put into service, then recital 97 suggests that model will be viewed as being placed on the market and the general-purpose AI model provisions will apply, in addition to those regarding AI systems. Those who integrate third party general-purpose AI models into their own AI systems are considered "downstream providers" and are granted certain rights under the AI Act. Recital 97 and other issues relating to the application of the general-purpose AI model rules (e.g. obligations for third parties who fine-tune a base model) are addressed in the Commission's Guidelines on the scope of obligations for providers of general-purpose AI models under the AI Act.

See Chapter 5 of this guide for more detail.

Territorial scope

AI System provisions

The AI Act has a broad jurisdictional scope for its AI system provisions: these are engaged when an AI system, either on its own or as part of a product covered by the EU product safety legislation in Annex I, is:

- placed on the EU market, put into service in the EU, imported into or distributed in the EU; or
- used by a deployer who has their place of establishment or is located in the EU.

The first point applies irrespective of where the provider of the AI system is established.

In addition to those cases, the AI system provisions also apply when outputs produced by an AI system outside are used in the EU, e.g. when a deployer located outside the EU uses outputs from a high-risk AI system within the EU. In that case, the non-EU established/located providers and deployers will also be caught by the scope of the AI Act. Recital 22 clarifies that in those instances the AI Act will apply even though the relevant AI systems are not placed on the market, put into service or used in the EU.

Prohibited AI Practices

The AI Act's provisions relating to prohibited AI practices apply to the placing on the EU market, putting into service in the EU and use of the AI practices set out in article 5. As we saw above, the definitions of *"placing on the market"* and *"putting into service"* refer to the EU market. The AI Act itself does not specify what a prohibited *"use"* would entail. The Commission's Guidelines on prohibited AI practices suggest that use *"should be understood in a broad manner to cover the use or deployment of the system at any moment of its lifecycle after having been placed on the market or put into service"* and further that use *"may also cover the integration of the AI system in the services and processes of the person(s) making use of the AI system, including as part of more complex systems, processes or infrastructure."*

General-purpose AI Models

The AI Act's general-purpose AI model provisions will be engaged where a provider of a general-purpose AI model places it on the market in the EU irrespective of where the provider is located or established. Section 3.1.2 of the Commission Guidelines on the scope of obligations for providers of general-purpose AI models provides nine examples of how a general-purpose AI model may be placed on the market.

Where can I find this?

Territorial Scope article 2 recitals 9-11

Exclusions

Certain activities are entirely outside the AI Act's scope. The AI Act does not apply to:

- areas outside the scope of EU law (e.g. activities concerning national security). This is the case irrespective of the type of entity entrusted under national legislation with carrying out the exempted activities. Given the very broad competences of the EU, as set out in the TFEU, this provision will have very limited scope of application in practice;
- AI systems placed on the market, put into service, or used with or without modification or where the AI system's output is used in the EU, exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities. An AI system placed on the market or put into service for an excluded purpose (military, defence or national security) and one or more non-excluded purposes (e.g. civilian purposes or law enforcement) is subject to the AI Act and providers of those systems should ensure compliance with the AI Act;
- public authorities in a third country or international organisations that use AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the EU or EU Member States, provided that such a third country or international organisation provides adequate safeguards for the protection of fundamental rights and freedoms of individuals. The national authorities and EU institutions, bodies, offices and agencies making use of those outputs remain subject to EU law;
- AI systems and models, including their output, specifically developed and put into service for the sole purpose of scientific research and development;
- research, testing or development of AI systems or models prior to their being placed on the market or put into service, excluding testing in real world conditions;
- deployers who are individuals and use the AI system in the course of a purely personal, non-professional activity. This is similar to the GDPR's *"household exemption"* – whilst providers of those AI systems continue to be subject to the AI Act; and
- AI systems released under free and open-source licences, unless they are placed on the market or put into service as high-risk AI systems, as a prohibited AI system or as a system that is covered by the Act's transparency obligations.

Relationship with other regulatory frameworks

- As a Regulation, the AI Act is directly applicable in EU Member States without the need for implementing legislation. EU Member States are prevented from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by the AI Act. This is only provided for in limited circumstances: for example, EU Member States may introduce more restrictive laws on the use of remote biometric identification systems – some of which constitute prohibited AI practices (article 5(5)) and the use of post-remote biometric identification systems, which constitute high-risk AI systems (article 26(10)).
- The AI Act's provisions on high-risk AI systems are built around the New Legislative Framework for EU products. This is a legislative package that sets out rules for the placing of products on the EU market, enhances market surveillance rules and rules for conformity assessments and CE marking. It also establishes a common legal framework for industrial products in the form of a toolbox of measures for use in future legislation. The AI Act specifies how these tools set out in the New Legislative Framework should apply in the context of AI systems.
- In parallel, the AI Act complements EU harmonisation legislation – this is the set of EU product safety legislation on the basis of which certain AI systems are to be classified as high-risk.
- The obligations of the AI Act apply in addition to and without prejudice to the obligations under GDPR, the e-Privacy Directive and the Law Enforcement Directive.

Prohibited AI Practices

At a glance

- Article 5 lists eight prohibited practices which are deemed to pose an unacceptable level of risk.
- Prohibitions came into effect on 2 February 2025.
- The prohibited practices are:
  - Subliminal, manipulative, or deceptive techniques.
  - Techniques exploiting vulnerable groups in each case which materially distorts behaviour and risks significant harm.
  - Social scoring in certain use cases.
  - Predicting criminality based on profiling.
  - Scraping the web or CCTV for facial recognition databases.
  - Inferences of emotions at workplaces or schools.
  - Biometric categorisation to infer race, political opinion, trade union membership, religious or political beliefs, sex life or sexual orientation.
  - Real-time remote biometric identification in public spaces for law enforcement purposes.
- Many of the prohibitions have exceptions – case by case analysis is needed.
- The list is not final: it will be re-assessed annually.
- Non-compliance is sanctioned by fines up to €35 million or 7% of total worldwide annual turnover for the proceeding financial year (whichever is higher).
- The prohibitions are operator-agnostic and apply irrespective of the role of the actor (i.e. whether provider, deployer, distributor or importer).

To do list

- [ ] Check the AI systems you use to see if they fall under the prohibited category.
- [ ] Check for updates to this list annually as the list of prohibited practices may change over time.
- [ ] Consider whether any exceptions apply. The prohibited practices are not absolute; many have exceptions.

Prohibited AI practices

The AI Act relies on a risk-based approach, so different requirements apply in accordance with the level of risk. This chapter concentrates on prohibited practices i.e. those which conflict with the values of the EU and are a clear threat to fundamental rights such as freedom, equality and privacy. The prohibitions are an attempt by law makers to respond to transparency and ethics concerns and to guarantee the protection of human rights.

The prohibited practices are listed exhaustively in article 5 (and are further explained in recitals 28 – 45 and by guidelines issued by the Commission on 4 February 2025) and provide a clear framework for what AI systems can and cannot do within the EU. The prohibitions in article 5 have applied since 2 February 2025 and were therefore the first provisions to come into force, highlighting their importance.

The list of prohibited practices in article 5 is exhaustive, but not final. The Commission will assess the need for amendment of the list of prohibited practices annually (article 112) and can submit findings to the European Parliament and Council. So, there may be variations to the list of prohibited practices in due course.

There are currently eight prohibited practices, which focus on practices that materially distort peoples' behaviour, or raise concerns in democratic societies. Special attention has been given to biometric identification systems. However, there are detailed exceptions to many of the prohibitions and each practice should be considered on a case-by-case basis.

Article 5(1)(a) Subliminal, manipulative or deceptive techniques

The first prohibition concerns AI systems deploying subliminal, manipulative or deceptive techniques in cases where:

- the techniques either aim to, or actually have, the effect of materially distorting the behaviour of an individual or a group;
- by appreciably impairing the ability of individuals to make informed decisions; and
- causing them to take decisions they would not otherwise have taken, and that either cause or are reasonably likely to cause them significant harm.

The techniques expressly mentioned in recital 29 involve: deployment of subliminal components such as audio, image, video stimuli that persons cannot perceive, or other manipulative or deceptive techniques that subvert or impair a person's autonomy, decision-making, or free choice, in ways so that people are not consciously aware of those techniques or, where they are aware of them, can still be deceived or are not able to control or resist them. The reference in recital 29 to machine-brain interfaces having the capability to materially distort human behaviour in a significantly harmful manner may also be the AI Act's attempt to regulate tools that employ neural data which is currently under discussion in other jurisdictions such as Colorado, California, and Chile.

For an AI system to be prohibited, there needs to be a causal link between the deceptive techniques and the significant harm caused. The threshold of *"significant"* harm was added in the legislative process and makes clear that not all dark patterns would fall under this provision.

The provision is open for interpretation and, in particular, the word "deceptive" will lead to further discussions. According to the Commission's guidelines, deceptive techniques could cover presenting false or misleading information with the objective or effect of misleading individuals, if the other requirements of the first prohibition are met.

Article 5(1)(b) Exploitation of vulnerabilities

The second category of prohibited AI practices aims to protect vulnerable people. There are three groups: vulnerability due to age, disability, or due to specific social or economic situations.

An AI system is only prohibited if it has the objective or the effect of materially distorting the behaviour of an individual and does so in a manner that causes or is likely to cause someone significant harm.

According to the Commission's guidelines on prohibited practices, exploitation based on socio-economic vulnerability does not arise where the relevant situation could be experienced by any person, regardless of their socio-economic status (for example, general feelings of grievance or loneliness). However, in such circumstances, the use of AI may still

fall within the separate prohibition in Article 5(1)(a) if it involves subliminal, manipulative or deceptive techniques that materially distort behaviour and cause significant harm.

AI systems that inadvertently impact socio-disadvantaged groups due to biased training data do not automatically exploit vulnerabilities, as there is no intentional targeting. However, under the Commission guidelines on prohibited practices, if AI providers or deployers are aware that their systems unlawfully discriminate against socio-economically disadvantaged persons and foresee significant harm without taking corrective action, they may still be considered to exploit these vulnerabilities.

An exploitation of a person's economic situation may arise where an AI system is used to identify individuals living in poverty and to take advantage of their financial vulnerabilities. Organisations that use AI systems for marketing, sales or similar activities should therefore ensure that their systems are assessed and tested to avoid targeting or exploiting individuals on this basis.

The concept of significant harm is common to both subliminal techniques and exploitation of vulnerable groups. In the legislative process, requirements that the harm needed to be physical or psychological were dropped. It therefore seems that a broad approach is intended to be taken to the concept of harm, although recital 29 still gives the examples of important adverse impacts on physical and psychological health, alongside financial interests. The recital also notes that harms can be accumulated over time.

This prohibition is not intended to affect lawful medical treatment (e.g. psychological treatment of a mental disease carried out with consent). Recital 29 also implicitly recognises that advertising and some other commercial practices inherently depend on nudging. It states that the intent is not to prohibit common, legitimate and lawful commercial practices, particularly in the field of advertising.

Furthermore, the key focus is on prohibiting manipulative techniques whilst persuasive approaches are not intended to be in scope. The Commission Guidelines on prohibited artificial intelligence practices differentiates as follows: "*In persuasive interactions, individuals are aware of the influence attempt and can freely and autonomously choose it. In manipulative interactions, the lack of awareness of the techniques or their impact negates the freedom of choice and informed and autonomous decision-making.*" Accordingly, consent can play a crucial role in these scenarios, as it ensures transparency with individuals being aware of the influence attempt thus respecting individual autonomy and user's free and informed choice to consent to the use of the AI system or not.

Article 5(1)(c) Social scoring

The third prohibition concerns so-called social scoring, i.e. classifying individuals or groups over a period based on their social behaviour, or known, inferred, or predicted personal characteristics. Social scoring is prohibited in two cases:

- if it leads to unfavourable treatment in social contexts that are unrelated to the context in which the data was originally generated; and
- if this leads to unfavourable treatment of individuals or groups that is unjustified or disproportionate to their social behaviour or its gravity.

Social scoring is often discussed in the context of government mandated systems which regulate access to public services, for example a scoring system based on socially accepted behaviour such as paying taxes on time or appearing to meetings set by an unemployment agency. The AI Act provision is even wider and encompasses social scoring systems in both public or private contexts. Many algorithms inherently depend on behavioural scores. However, the AI Act only prohibits those scoring systems which result in unfavourable treatment in unrelated social contexts. This key restriction targets the consequences of social scoring, preventing unjust outcomes, or discrimination of individuals or groups.

The social scoring prohibition under the AI Act therefore depends on the context the data has been obtained from and the context the data is being used in. As the Commission guidelines on prohibited practices illustrate, lawful activities, like credit and risk scoring in financial services, are permitted if they improve service quality or prevent fraud. Conversely, an insurance company using spending and other financial data from a bank to set life insurance premiums is provided as an example of unlawful social scoring.

Article 5(1)(d) Profiling for criminal risk assessment

Article 5(1) prohibits the placing on the market, putting into service, or using of AI systems that assess or predict the likelihood of a person committing criminal offences based solely on profiling or on assessing the personality traits and characteristics of a person. There is an exception for AI systems used to support human assessment of involvement of a person in a criminal activity, which is based on objective and verifiable facts directly linked to a criminal activity – i.e. detection tools which are factual and supplement, but do not supplant, human decision making. This prohibition seeks to prevent individuals from being subjected to adverse treatment or suspicion in the absence of concrete conduct (e.g. the type of system depicted in the film *Minority Report*). It reflects fundamental principles such as human dignity and the presumption of innocence, as protected by article 1 of the Charter of Fundamental Rights of the EU.

The Commission guidelines on prohibited practices emphasise that the prohibition can extend to private entities if they act with public authority or assist law enforcement. For instance, a private company analysing data for law enforcement might be within the scope of the prohibition if the relevant criteria are met.

The Commission guidelines also highlight that, where a system falls under the exclusion in article 5(1)(d) for AI systems that support the human assessment based on objective and verifiable facts directly linked to a criminal activity, it will still be classified as a high-risk AI system if it is intended to be used by law enforcement authorities or on their behalf.

Article 5(1)(e) Facial recognition databases

The fifth prohibited practice is the placing on the market, putting into service for the specific purpose, or use of AI systems to create or expand facial recognition databases through untargeted scraping of facial images from the internet or CCTV footage. Recital 43 considers this practice to add to the feeling of mass surveillance and that it can lead to gross violations of fundamental rights, including the right to privacy. This may be a response to the investigations by supervisory authorities into Clearview AI.

The Commission guidelines on prohibited practices regarding facial recognition databases clarify several key points. Most notably, such databases are prohibited regardless of whether they are temporary, centralised, or decentralised, and they fall under Article 5(1)(e), if they can be used for facial recognition, regardless of their primary purpose. Targeted scraping, such as collecting images of specific individuals or using reverse image searches, is allowed, but combining it with untargeted scraping is prohibited. The prohibition does not cover untargeted scraping of other biometric data, like voice samples, or databases not used for facial recognition, such as those for AI model training without identifying individuals.

Article 5(1)(f) Inference of emotions in working life and education

The sixth prohibited practice is the placing on the market, putting into service for this specific purpose, or use of AI systems to infer emotions in workplaces or educational institutions, except for safety or medical reasons. The Commission's guidelines clarify that the definitions of both educational institutions and workplaces should be interpreted widely and in the case of workplace use they should also cover the selection and hiring phases of recruitment. The exception for the safety or medical reasons on the other hand, is to be interpreted narrowly. For example, medial reasons cover therapeutic uses but not monitoring general wellbeing. As a result, systems intended to detect burnout or depression in the workplace would not be exempt.

The prohibition in article 5(1)(f) refers broadly to the use of AI systems to infer emotions, without expressly requiring that such inferences be based on biometric data. This is inconsistent with the AI Act defining *"emotion recognition systems"* as an AI system used to identify or infer the emotions or intentions of natural persons on the basis of biometric data. The Commission's guidelines clarify this apparent inconsistency by explaining that article 5(1)(f) should be interpreted as applying to *"emotion recognition systems"* as defined in the AI Act. On that basis, non-biometric emotion recognition systems (for example, systems analysing text alone) are not prohibited, provided they are not used in conjunction with biometric data. The rationale given for the prohibition is the inaccuracy and intrusive nature of biometric emotion recognition systems, particularly in contexts characterised by power imbalances, such as workplaces and educational institutions.

Recital 18 clarifies that the prohibition applies to emotions or intentions (such as happiness, sadness, anger etc), while the notion does not include physical states, such as pain or fatigue. Therefore, systems used in detecting the state of fatigue of professional pilots or drivers for the purpose of preventing accidents are not prohibited. It also does not cover the detection of readily apparent expressions such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering.

Article 5(1)(g) Biometric categorisation

The seventh prohibition is on the use of biometric categorisation systems that categorise individuals based on their biometric data to deduce or infer certain (not all) special category data under the GDPR, namely: race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.

Special category data under the GDPR that are not covered in the prohibition are inferences of ethnic origin, health, and genetic data. However, inferring such types of data would likely fall under the high-risk category according to No. 1(b) of Annex III. In addition, the prohibition does not extend to the labelling or filtering of lawfully acquired biometric datasets, nor to certain forms of biometric categorisation carried out by law-enforcement authorities, such as sorting images by hair or eye colour for investigative purposes. Recital 54 nevertheless indicates that AI systems intended for biometric categorisation based on sensitive attributes or special-category data, insofar as they are not prohibited by the AI Act, should generally be treated as high-risk. Consistent with this approach, the Commission's guidelines state that most AI systems falling within an exception to an article 5 prohibition will qualify as high-risk, suggesting that these exempted labelling and filtering systems will typically be subject to the high-risk regime.

Recital 16 clarifies that biometric categorisation systems do not include purely ancillary features which are linked to another commercial service, where the feature cannot, for objective technical reasons, be used without the main service, and where this is not a circumvention mechanism to evade AI Act rules (e.g. retail try before you buy filters, or social media filters).

The guidelines also clarify that the scope of biometric categorisation excludes categorisation according to clothes or accessories, such as scarfs or crosses, or social media activity.

Article 5(1)(h) Real-time remote biometric identification in public spaces for law enforcement

Lastly, article 5(1)(h) prohibits the use of real-time Remote Biometric Identification Systems (RBI) in publicly accessible spaces for law enforcement purposes. RBI systems are AI systems for the purpose of identifying natural persons, without their involvement, typically at a distance, by comparing biometric data with that contained in a reference database. Real-time systems include those where there is a short, insignificant delay in the comparison. The AI Act does not specify what constitutes a "*significant delay*". However, the Commission's guidelines indicate that a delay is likely to be considered significant where the individual has already left the location in which the biometric data was captured, such that the system no longer enables an immediate or near-immediate response by law-enforcement authorities.

Biometric systems used for verification—that is, to confirm that a person is who they claim to be in order to access a service, device or secure premises—are distinguished from RBI and are therefore not covered by this prohibition (recital 15). The Commission's guidelines explain that the key distinction between identification and verification lies in the active involvement of the individual in the verification process, which is considered to entail a more limited impact on fundamental rights. Active involvement requires more than merely informing individuals that cameras are present. Rather, the person must take a deliberate and conscious action to participate in the verification process, such as intentionally presenting themselves to a camera that is installed and designed in a way that clearly invites and facilitates such active participation.

The AI Act allows (but does not require) EU Member States to permit use of RBI for law enforcement purposes in limited situations where the use of RBI is strictly necessary for:

- targeted searches for specific victims of abduction, human trafficking, or sexual exploitation as well as searching for missing persons;

- the prevention of a specific, substantial, and imminent threat to the life or physical safety, or a genuine and present or foreseeable threat of terrorist attack; or

- the localisation or identification of a person suspected of having committed a criminal offence, conducting a criminal investigation, prosecution or executing a criminal penalty for those offences referred to in Annex II and punishable in the EU Member State concerned by a prison sentence for a maximum period of at least four years.

The exemptions permit the use of RBI only to confirm the identity of a specifically targeted individual. Any such use must be strictly necessary and proportionate, taking into account the nature of the situation, including the seriousness, likelihood and scale of the harm that would arise if the system was not used, balanced against the impact on the rights and freedoms of the persons concerned.

Additional safeguards apply, including the requirement to carry out a fundamental rights impact assessment, to register the system in the EU database in accordance with article 49, and to obtain prior authorisation for each use case from a judicial or administrative authority, subject to narrowly defined urgency exceptions. Each use of RBI in publicly accessible spaces must also be notified to the relevant market surveillance authority and national data protection authority. EU Member States are required to report this information to the Commission, which in turn publishes an annual report on the use of such systems.

To whom do the prohibitions apply?

As set out in Chapter 2, the AI Act distinguishes between different operators involved in AI systems, attributing specific responsibilities based on their role in relation to the AI model or system.

However, the rules on prohibited practices are operator-agnostic. In other words, they apply universally, independent of the specific role of the operator (i.e. whether they are involved in the provision, development, deployment, distribution, or use of AI systems engaging in prohibited practices).

Enforcement and fines

When a practice is prohibited, the AI system in question may not be used in the EU. In case of an infringement, competent authorities may issue a fine of up to 7% of the total worldwide annual turnover of the offender for the preceding financial year or €35 million, whichever is higher.

National market surveillance authorities will be responsible for ensuring compliance with the AI Act's provisions regarding prohibited AI systems. They will report to the Commission annually about use of prohibited practices that occurred during the year and about the measures they have taken.

Where can I find this?

Subliminal, manipulative or deceptive techniques	article 5(1)(a)	recitals 28 & 29
Exploitation of vulnerabilities	article 5(1)(b)	recitals 28 & 29
Social scoring	article 5(1)(c)	recital 31
Profiling for criminal risk assessment	article 5(1)(d)	recital 42
Facial recognition database	article 5(1)(e)	recital 43
Inference of emotions in working life and education	article 5(1)(f)	recitals 44 - 45
Biometric categorisation	article 5(1)(g)	recital 30
Real-time remote biometric identification in public spaces	article 5(1)(h)	recitals 32 - 41

Other useful resources

- Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU 2024/1689 (AI Act)
- ETHICS GUIDELINES FOR TRUSTWORTHY AI: High-Level Expert Group on Artificial Intelligence (2019)
- EDPB Guidelines on Processing Personal Data Through Video Devices
- EDPB Guidelines on Use of Facial Recognition Technology In The Area of Law Enforcement
- EDPB Guidelines on Automated Decision Making and Profiling
- EDPB-EDPS Joint Opinion On The Proposal For The Artificial Intelligence Act
- EDPB guidelines on Deceptive Design Patterns in Social Media
- Guidelines on dark patterns from the Finnish Market Authority

High-risk AI systems

At a glance

- AI systems are considered to be *"high-risk"* if they are intended to be used as:
  - products, or safety components of products, which must undergo third-party conformity assessment pursuant to the legislation covered by Annex I; or
  - for one of the purposes described in Annex III.
- Providers, deployers, importers, distributors and suppliers to providers of high-risk AI systems have obligations under the AI Act. A single entity may perform more than one role in relation to a high-risk AI system and must comply with the corresponding obligations for each role in parallel.
- Providers of high-risk AI systems have the heaviest compliance burden and need to carry out a conformity assessment before the system can be placed on the market or put into service.
- It's possible to become the provider of a high-risk AI system (e.g. by placing your own name/trademark on the system, making a substantial modification, or using the system for different purposes than intended by the original provider).

To do list

- [ ] Determine whether the AI system qualifies as a high-risk as meant in article 6, taking into account Annexes I and III.
- [ ] Determine your role in the value chain (provider, deployer, importer, distributor, or third-party supplier) and review the corresponding obligations.

Classification of an AI system as a high-risk AI system

High-risk AI systems are those that can have a significant harmful impact on the health, safety and fundamental rights of persons in the EU. There are two main categories of high-risk AI systems:

a. systems which are intended to be used as safety components of products or systems, or which are themselves products or systems, falling within the scope of EU harmonisation legislation listed in Annex I, if required to undergo a third-party conformity assessment pursuant to this legislation; and

b. systems whose intended purpose falls within the scope of the use cases set out in Annex III.

Category A: Annex I systems

Regarding the first category (a), the product safety legislation listed in Annex I covers the following categories, divided into two Sections:

Section A

- machinery
- toys
- recreational craft and personal watercraft
- lifts/elevators
- equipment and protective systems for potentially explosive atmospheres
- radio equipment
- pressure equipment
- cableway installations
- personal protective equipment
- appliances burning gaseous fuels, medical devices
- in vitro diagnostic medical devices

Section B

- civil aviation
- 2/3-wheel vehicles
- agricultural and forestry vehicles
- marine equipment
- rail systems
- motor vehicles and their trailers
- unmanned aircraft

Section A lists EU harmonisation legislation under which AI systems that are products or safety components and are subject to third-party conformity assessment are classified as high-risk and must comply with the full set of high-risk requirements under the AI Act. Section B covers sectors subject to established safety regimes, such as aviation and rail, where AI systems are also treated as high-risk but only a limited subset of AI Act obligations applies, and no additional AI-specific conformity assessment is required beyond the applicable sectoral framework.

The legislation in Annex I covers the categories listed above but can also cover related products. For example, the Machinery Regulation covers lifting accessories and removable mechanical transmission devices as well as machinery itself. It's also the core regulation for robotics, where AI is also steadily adopted, so that the AI Act and its high-risk requirements will become highly relevant.

Safety components fulfil a safety function for a product, where their failure or malfunction would endanger the health and safety of persons or property. Whether an AI system qualifies as a high-risk AI system therefore depends on an assessment under the applicable product safety legislation listed in Annex I, in particular on whether that legislation requires the system to undergo a third-party conformity assessment. For example, in the Medical Device Regulation, medical devices in class IIa and higher are subject to the third-party conformity procedure. If an AI-system qualifies as a safety component

of such a medical device, or if it constitutes such a medical device itself, it is a high-risk AI system pursuant to the AI Act.

Some of the legislation covered in Annex I also uses terms such as "high-risk" and "medium-risk". However, these categories are independent from the classification as high-risk under the AI Act. For example, under applicable product safety legislation a product can be classed as "medium-risk", but if the product has to undergo third-party conformity assessment, then an AI system that is a safety component of that product, or that itself constitutes such a product, will be high-risk under the AI Act.

Category B: Annex III systems

The stand-alone list of high-risk systems currently contains:

- **Biometrics:** remote biometric identification of individuals, biometric categorisation of individuals and/or emotion recognition of individuals.
- **Management and operation of critical infrastructure:** AI systems intended to serve as safety components in the management and operation of critical digital infrastructure (e.g., internet exchange points, DNS services, TLD registries, cloud computing services, data centres, content delivery networks, trust service providers, electronic communication networks or services), road traffic, or in the supply of water, gas, heating or electricity are high-risk and thus subject to strong regulation to directly protect physical integrity or health and safety of individuals and property.
- **Education and vocational training:** decision-making in education and vocational training (e.g. selection, evaluation, assessment and monitoring of students or individuals applying to be students).
- **Recruitment and HR:** decision-making in recruitment and HR (e.g. selection, evaluation, assessment, promotion, termination, task allocation and monitoring of employees and/or other workers and/or applicants).
- **Essential services:** evaluating the (continued) eligibility of individuals for public assistance benefits (e.g. healthcare services, social security allowances, disability benefits); evaluating creditworthiness of individuals or establishing their credit score (with the exception of the detection of financial fraud); risk assessment and pricing in relation to individuals in the case of life and health insurance; and evaluating and classifying emergency calls or making decisions in relation to dispatching or prioritisation of the dispatching of emergency first response services (e.g. police, firefighters, medical aid); and emergency healthcare patient triage.
- **Crime analytics:** assessment by/on behalf of/in support of law enforcement authorities: (i) of the risk of individuals of becoming a victim or (re-)offender; (ii) of personality traits and characteristics; (iii) of past criminal behaviour of individuals or groups; or (iv) consisting of profiling of persons, in the course of the detection, investigation or prosecution of criminal offences.
- **Evidence gathering and evaluation:** evaluation of reliability of evidence during the investigation or prosecution of criminal offences, or in the course of applications for asylum, visa or residence permits, or with regard to associated complaints; use of polygraphs or similar tools by/on behalf of/in support of law enforcement authorities or authorities conducting migration, asylum and/or border control.
- **Immigrant identification, migration risk and migration application assessment:** detecting, recognising or identifying individuals (with the exception of verification of travel documents) in the context of migration, asylum or border control management; assessment of risk (e.g. security risk, risk of irregular migration or health risk) posed by individuals who intend to enter or have entered the territory of an EU country and examination of applications for asylum, visa or residence permits and for associated complaints.
- **Administration of justice:** assisting judicial authorities or alternative dispute resolution institutions in researching and interpreting facts and the law and in applying the law to facts.
- **Democratic processes:** influencing the outcome of an election or referendum or voting behaviour of individuals.

Note that Annex III may be amended by the Commission (article 7).

The intended purpose of an AI system is defined in article 3(12) as: *"the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation."* The concept of *"intended purpose"* under the AI Act closely mirrors the approach taken under EU medical device law, where regulatory classification depends primarily on the manufacturer's stated intention as evidenced by instructions for use, promotional materials and technical documentation, rather than on the product's theoretical capabilities or unintended downstream uses.

Exceptions: not sufficiently high-risk

Article 6(3) provides that AI systems shall not be considered high-risk under certain conditions, even if their intended purpose falls within the scope of Annex III, so that they would be high-risk (absent the exceptions). This is the case, if the AI system does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons. The article mentions four criteria. The exceptions can be relied upon if one or more of these criteria are fulfilled (article 6(3) and recital 53):

- the AI system is intended to perform a narrow procedural task;
  - Example: a system which transforms unstructured data into structured data or a system which detects duplicates of documents.
- the AI system is intended to improve the result of a previously completed human activity;
  - Example: a system which improves the professional tone or academic style of language used in already drafted documents.
- the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
  - Example: a system which checks flags inconsistencies or anomalies in the grades applied by a teacher, when compared with an existing grading pattern for that teacher.
- the AI system is intended to perform a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III.
  - Example: a system for translating documents.

The exception does not apply if the AI system involves profiling of natural persons within the meaning of article 4(4) of Regulation (EU) 2016/679 (GDPR) or article 3 (4) of Directive (EU) 2016/680 (Data Protection Enforcement Directive) or article 3, (5) of Regulation (EU) 2018/1725 (Data Protection for EU institutions) (recital 53).

Companies deciding to make use of this exception should note that they carry the burden of proof as to whether the system is high-risk. The assessment under article 6(3) must be documented before the system is placed on the market or put into service and the system must be registered (articles 49(2) and 6(4)). Providers of such systems must provide this documentation to national competent authorities on request.

The Commission is due to provide guidelines specifying the practical implementation of article 6, including a comprehensive list of practical examples of high-risk and non-high-risk use cases of AI systems. These guidelines were due by 2 February 2026 (article 6(5)). It may also adopt delegated acts adding to or modifying the criteria for article 6(3).

Obligations for providers of high-risk AI systems

The AI Act provides a detailed list of obligations for providers and deployers of high-risk AI systems as follows in Chapter III, Sections 2, 3 and 4:

Obligations for providers on high-risk AI systems	
Requirements of Section 2	Ensure compliance with requirements of Section 2 (see below).
Name of provider and contact information	Indicate on the AI system (or, if not possible, on its packaging or accompanying documentation) the name of the provider or its brand and its contact information.
Quality management system	Have a quality management system complying with article 17 (article 17 provides a detailed list of aspects of the AI system to be documented through policies, procedures and instructions).
Documentation	Keep the documentation referred to in article 18. The documentation will include: • technical documentation (article 11). • documentation concerning the quality management system (article 17). • documentation concerning changes approved by notified bodies, where applicable. • decisions and other documents issued by notified bodies, where applicable. • the EU declaration of conformity (article 47).
Logs	If the AI system is under their control, keep logs automatically generated by the AI system (article 19). Such logs must be kept for a period appropriate to the intended purpose of the high-risk AI system. The period should be at least six months (unless any personal data protection provisions state otherwise).
Conformity Assessment	Ensure that the AI system undergoes the relevant conformity assessment procedure in article 43, prior to being placed on the market or put into service (see below).
Declaration of conformity	Draw up an EU declaration of conformity (article 47). See below.
CE marking	Affix the CE marking to the AI system (or, if not possible, on its packaging or accompanying documentation). The CE marking will confirm the conformity of the high-risk AI system with the AI Act as per article 48. See below.
Registration obligation	Comply with EU Database registration obligations (article 49(l)). See below.

Corrective actions/ provision of information	In cases where the AI system is not in conformity with the AI Act, take the necessary corrective actions, or withdraw, disable, or recall it. Where the AI system presents a risk to safety, or the fundamental rights of persons, inform the competent market surveillance authorities and, where applicable, the notified body that issued a certificate for that system (article 79).
Demonstration of conformity	Upon a reasoned request of a national competent authority, demonstrate the conformity of the AI system with the requirements set out in Section 2 (see above), providing all necessary information and documentation. The duties relating to cooperation with competent authorities are set out in more detail in article 21. Any information shared with a national competent authority shall be treated as confidential.
Accessibility requirements	Ensure the AI system complies with accessibility requirements in accordance with: • 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).

Harmonised standards and conformity assessment procedure for providers of high-risk AI systems

Harmonised standards

If the AI system complies with harmonised standards, there will be a presumption of conformity with the requirements for high-risk AI systems in Chapter III, Section 2 (article 40(1). Harmonised standards will be published in the Official Journal of the European Union.

Harmonised standards are highly relevant in practice. Under traditional product safety laws, 'manufacturers' usually follow them to demonstrate compliance with product safety law requirements. This will be similar under the AI Act.

The Commission issued a (draft) standardisation request in accordance with article 40(2) to standardisation bodies CEN/CELENEC, requesting these bodies to draft harmonised standards covering the requirements of Chapter III, Section 2 by 30 April 2025 (see also Chapter 9).

Conformity assessment procedure

The conformity assessment procedure for high-risk AI systems under article 43 requires providers to demonstrate compliance with the requirements for high-risk AI systems in Section 2 of Chapter III (overview below).

Annex III high-risk AI systems

The AI Act provides for two main conformity assessment procedures for high-risk AI systems. As a general rule, providers of high-risk AI systems listed in points 2 to 8 of Annex III must apply the internal control procedure set out in Annex VI, without the involvement of a notified body.

High-risk AI systems listed in point 1 of Annex III (biometric systems) are subject to a differentiated regime. Where the provider has applied harmonised standards or common specifications in accordance with articles 40

and 41, the internal control procedure under Annex VI is sufficient. However, where such standards or specifications have not been applied, the conformity assessment must involve a notified body.

Annex I high-risk AI systems

If a high-risk AI system falls under EU harmonisation legislation listed in Section A of Annex I, the conformity assessment procedures from those legal acts apply. The high-risk AI system requirements of Section 2 in Chapter III are integrated into this assessment, and specific provisions of Annex VII also apply. Notified bodies under these legal acts must comply with certain requirements of the AI Act, to ensure consistent oversight. By contrast, where a high-risk AI system falls under EU harmonisation legislation listed in Section B of Annex I, the AI Act does not introduce additional or separate conformity assessment procedures, and compliance with the applicable AI Act requirements is addressed exclusively through the existing sector-specific regulatory and oversight frameworks.

New conformity assessments for substantial modifications

Substantial modifications to high-risk AI systems necessitate a new conformity assessment. However, changes that form part of the system's predetermined learning process do not count as substantial modifications.

Requirements for high-risk AI systems

Focus on Articles 8-15; requirements for high-risk AI systems	
Compliance with the requirements (article 8)	Article 8 emphasises that high-risk AI systems must meet technical and organisational requirements (articles 9-15) throughout their life cycle, considering the intended use and the status of the technology. It's crucial to prioritise requirements impacting humans and if suitable trade-offs are not found, the AI system should not be deployed.
Risk management (article 9)	Article 9 requires providers to establish a risk management system. This is an ongoing process to identify, analyse, and mitigate foreseeable risks, including designing risk reduction measures, implementing controls, and providing user information and training. The measures taken must be documented and high-risk AI systems tested at appropriate stages to ensure consistent performance.
Data governance (article 10)	Robust data governance is a critical component of the technical and organisational requirements for high-risk AI systems. High-quality, representative, and to the best extent possible error-free and complete training, validation, and testing datasets are required to ensure proper functioning and safety of the system. Providers must also take measures to mitigate biases in datasets that could lead to prohibited discrimination, including by processing special categories of personal data under specific conditions. Certified third-party services can be employed for data integrity verification and to demonstrate compliance with the AI Act's data governance requirements.
Technical documentation and record keeping (articles 11 and 12)	Articles 11 and 12 necessitate detailed technical documentation and record-keeping logs throughout the system's lifecycle. Providers must prepare this before deployment and regularly update it. It should cover all aspects of the system, including its characteristics, algorithms, data, training, testing, validation, and risk management. High-risk AI systems should also automatically record usage logs to provide traceability and identify potential risks or needed modifications.

Transparency and provision of information (article 13)	Article 13 mandates clear, comprehensive instructions for deployers of high-risk AI systems. These instructions should enable deployers to understand and use the AI system's outputs correctly. The AI system's decision-making must be understandable, and details on its identity, characteristics, limitations, purpose, accuracy, risks, capabilities, oversight, maintenance, and expected lifespan must be provided. All documentation should be tailored to the needs and knowledge level of the intended deployers.
Human oversight (article 14)	Human oversight measures must prevent or minimise risks to health, safety, and rights. These measures must be proportionate to the AI system's risks and level of autonomy. Human operators should also be able to override the system if necessary. Oversight can be achieved through: • Built-in system constraints and responsiveness to human operators. • Provider-identified measures for deployers to help them make informed, autonomous decisions. • Oversight approaches can include human-in-the-loop, human-on-the-loop, or human-in-command, depending on the application's risks.
Accuracy, robustness and cybersecurity (article 15)	Article 15 mandates that high-risk AI systems must achieve suitable accuracy, robustness, and cybersecurity levels. Accuracy measures include minimising prediction errors, robustness measures ensure systems can handle errors and inconsistencies. Lastly, cybersecurity measures shall protect against unauthorised system alterations in which case compliance can be demonstrated through compliance with the EU Cyber Resilience Act for relevant AI systems subject to the EU Cyber Resilience Act.

Obligations for deployers of high-risk AI systems

The AI Act provides for obligations for deployers of high-risk AI systems (article 26):

Technical and organisational measures

Deployers must take appropriate technical and organisational measures to ensure they use such systems in accordance with the instructions for use accompanying the systems.

Human oversight

Deployers must assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support.

Input data

Where the deployer exercises control over input data, that deployer must ensure that the input data is relevant and sufficiently representative. In other words, this principle states the deployer's responsibility as to the quality of the input data.

Monitoring high-risk AI system

Deployers must monitor the operation of the high-risk AI system based on the instructions for use. If the deployer identifies that using the AI system in accordance with its instructions presents a risk to the health or safety, or to fundamental rights, it must, without undue delay, inform the provider or distributor and the relevant market surveillance authorities

and suspend the use of that system. If a serious incident is identified, deployers must also immediately inform the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident. These deployer obligations are intended to align with the provider's post-market monitoring obligations (article 72) and incident reporting obligations (article 73).

Logs

Deployers of high-risk AI systems must keep logs automatically generated by that high-risk AI system where these logs are under their control. The logs must be kept for a period appropriate to the intended purpose of the high-risk AI system. This period is at least six months, unless provided otherwise in applicable EU or national law, in particular on the protection of personal data.

Information to the workers' representatives

Deployers who are employers must inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system.

Public authority deployers

Deployers of high-risk AI systems who are public authorities, or EU institutions, bodies, offices or agencies must comply with the EU Database registration obligations under article 49.

Data protection impact assessment

If deployers of high-risk AI systems are required to perform a data protection impact assessment under article 35 of Regulation (EU) 2016/679 (GDPR) or article 27 of Directive (EU) 2016/680 (Data Protection Enforcement Directive), they must make use of the information provided by the provider under article 13.

Information to affected individuals

Deployers of high-risk AI systems listed in Annex III that make decisions, or assist in making decisions, relating to natural persons must inform the individuals concerned that they are subject to the use of a high-risk AI system. This obligation for deployers of high-risk AI systems applies in addition to any applicable transparency obligations under article 50.

Investigation for criminal offences – high-risk AI system for post-remote biometric identification

Without prejudice to Directive (EU) 2016/680 (Data Protection Enforcement Directive), in the framework of an investigation for the targeted search of a person suspected or convicted of having committed a criminal offence, someone who wishes to deploy a high-risk AI system for post-remote biometric identification must request an authorisation for this use, ex-ante, or without undue delay and no later than 48 hours, from a judicial authority or an administrative authority.

Fundamental rights impact assessment for high-risk AI systems

Article 27 requires certain deployers to carry out a fundamental rights impact assessment (FRIA) before deploying a high-risk AI system listed in Annex III (with the exception of safety components in the management and operation of critical infrastructure under Annex III, point 2). This obligation applies to deployers who are bodies governed by public law and private entities providing public services, as well as to any deployer of high-risk AI systems used for creditworthiness assessment or for risk assessment and pricing in relation to life and health insurance.

The assessment consists of:

- a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose;
- a description of the time period within which, and the frequency with which, each high-risk AI system is intended to be used;
- the categories of natural persons and groups likely to be affected by its use in the specific context;

- the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified, considering the information given by the provider pursuant to article 13;
- a description of the implementation of human oversight measures, according to the instructions for use; and
- the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.

Obligations for other operators in connection with high-risk AI systems

Most obligations regarding high-risk systems in the AI Act are directed at providers and deployers. However, there are also a limited set of obligations for other operators: namely, importers and distributors of high-risk AI systems, and suppliers of any systems, tools, services, components or processes which are used or integrated in high-risk AI systems. Examples of services by suppliers include model (re)training, testing and evaluation and integration into software (recital 88). The obligations do not apply to suppliers that offer the relevant product or service under a free and open-source licence (article 25(4)). Additionally, it is possible for operators other than the original provider of an AI system to be assigned the role of provider of a high-risk AI system by the AI Act.

Obligations for importers, distributors and suppliers

Articles 23, 24 and 25(4) set out the obligations for importers, distributors and suppliers:

Importers (article 23)	Distributors (article 24)	Suppliers (article 25(4))
Verification: before placing the AI system on the market, verifying that the provider has genuinely: • carried out the appropriate conformity assessment procedure; • drawn up the required technical documentation; • affixed the CE marking and drawn up the EU declaration of conformity; and • appointed an authorised representative.	**Verification:** before making the AI system available on the market, verifying that: • it bears the CE marking; • it is accompanied by a copy of the EU declaration of conformity and instructions for use; and • the provider and the importer, as applicable, have complied with their respective obligations.	**Provide assistance:** by written agreement, specifying the necessary information, capabilities, technical access and other assistance based on the generally acknowledged state of the art, in order to enable the provider of the high-risk AI system to fully comply with their obligation. The AI Office may also develop and recommend voluntary model contractual terms between providers of high-risk AI systems and their third-party suppliers (article 25(4)) and recital 90).
Risk flagging: an importer must (i) not place a high-risk AI system on the market where they have sufficient reason to consider that it is not in conformity with the AI Act, is falsified, or is accompanied by falsified documentation until the AI system has been brought into conformity, and (ii) inform the provider, the authorised representative and the market surveillance authority when the system presents a risk[1] to health, safety or fundamental rights of persons.	**Risk flagging**: a distributor must (i) not make the AI system available when the distributor considers or has reason to consider that the AI system is not in conformity with the requirements set out in Section 2, until the AI system has been brought into conformity, and (ii) where the AI system presents a risk to health, safety or fundamental rights of persons, immediately inform the provider or the importer of the AI system.	
Care: ensure that storage or transport conditions do not jeopardise compliance with the requirements in Section 2.	**Care:** ensure that storage or transport conditions do not jeopardise compliance with the requirements in Section 2.	

1. Risk here means: *"having the potential to affect adversely health and safety of persons in general, health and safety (…) 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 of the product concerned, including the duration of use and, where applicable, its putting into service, installation and maintenance requirements"* (article 79(1) AI Act in conjunction with Article 3(19) of Regulation (EU) 2019/1020 (Market surveillance regulation).

Importers (article 23)	Distributors (article 24)	Suppliers (article 25(4))
Cooperation with authorities: upon a reasoned request, provide competent authorities with all necessary information/ documentation, including technical documentation, to demonstrate conformity of the AI system and cooperate with these authorities in any action they take in relation to the system. **Record keeping:** keep, for a period of ten years after the AI system has been placed on the market/put into service, a copy of the certificate issued by the notified body (if there has been a third-party conformity assessment), the instructions for use and the EU declaration of conformity. **Contact details:** indicate name, registered trade name or registered trademark and the address at which the importer can be contacted on the system and its packaging or accompanying documentation.	**Cooperation with authorities:** upon a reasoned request, provide competent authorities with all necessary information/documentation regarding their obligations in the rows above to demonstrate the conformity of that AI system, and cooperate with these authorities in any action they take in relation to the AI system. **Corrective actions:** take the corrective actions necessary to bring the AI system into conformity, where the distributor considers or has reason to consider the AI system not to be in conformity with the requirements set out in Section 2, or withdraw or recall the AI system, or ensure that the provider, the importer or any relevant operator, as appropriate, takes those corrective actions.	

Becoming a provider of someone else's (high-risk) AI system

Article 25(1) provides that a person will be considered the provider of a high-risk AI system, even if that person was not originally the provider of the AI system, when that person:

- places their name or trademark on a high-risk AI system which is already placed on the market or put into service;
- makes a substantial modification[2] to an existing high-risk AI system in such a way that it remains high-risk; and/or
- modifies the intended purpose of an AI system which is not currently high-risk so that it becomes high-risk.

If any of these three situations occur, the original provider will no longer be considered the provider of the (new or newly used) AI-system.

2. A 'substantial modification' is defined in article 3(23) as "a change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider and as a result of which the compliance of the AI system with the requirements set out in Chapter III, Section 2 is affected or results in a modification to the intended purpose for which the AI system has been assessed". The Commission will provide further guidelines on the practical implementation of the provisions related to substantial modification (Article 96(1)(c)). Recital 84 also provides that provisions established in certain EU harmonisation legislation based on the New Legislative Framework, such as the Medical Device Regulation, should continue to apply. For example, article 16(2) of the Medical Device Regulation provides that certain changes should not be modifications of a device that could affect its compliance with the applicable requirements, and these provisions should continue to apply to high-risk AI systems which are medical devices within the meaning of the Medical Device Regulation.

Instead, the person that caused any of these three situations to occur will be the provider of that high-risk AI system.

One situation which often occurs in practice that could lead to such switching of provider roles is the deployment of a general-purpose AI system by a deployer in a way that falls within the high-risk category as set out in article 6 (and Annexes I and III). As such, if a person deploys a general-purpose AI system in a high-risk way (i.e. modifies its intended purpose to a high risk one), that deployer then becomes the provider.

The new provider will assume all the obligations of a provider of a high-risk AI system. The original provider is obliged to closely cooperate with the new provider and make available the necessary information and provide reasonably expected technical access and other assistance to the new provider to bring the AI system into conformity with the AI Act (article 25(2)). If, however, that original provider had "clearly specified" that the AI system was not to be changed into a high-risk AI system (article 25(2)) or "expressly excluded the change of the AI system into a high-risk AI system" (recital 86), for example by prohibiting deployment for high-risk purposes in the applicable contract(s), then that original provider is not obligated to assist the new provider with compliance. If high-risk deployment is not prohibited, then the co-operation obligation applies, but is without prejudice to the need to observe and protect intellectual property rights, confidential business information and trade secrets.

Where can I find this?

Scope of high-risk systems	article 6, Annexes I and III	recitals 46-63
Requirements for providers of high-risk AI systems	articles 8-22, 43, 47-49	recitals 64-83, 123-128, 147, 131
Requirements for deployers of high-risk AI systems	article 26, 27	recitals 91-96
Requirements for importers of high-risk AI systems	article 23	recitals 83
Requirements for distributors of high-risk AI systems	article 24	recitals 83
Requirement for third-party suppliers to high-risk systems	article 25	recitals 83-90
Standards	article 40, 41	recital 121
Conformity assessment procedure	article 28	recital 149

General-purpose AI models

At a glance

- General-purpose AI (GPAI) models are AI models designed with a high degree of generality, capable of competently performing a wide range of distinct tasks, including (but not limited to) current large generative AI models.
- Providers of general-purpose AI models are tasked with a number of transparency obligations both towards the AI Office and competent authorities as well as towards AI systems providers intending to integrate the general-purpose AI model into their AI system. They are also required to put in place a policy to comply with EU law on copyright and related rights and to draw up and make publicly available a sufficiently detailed summary about the content used for training.
- General-purpose AI models that pose systemic risks, i.e., the most versatile and powerful models, are under heightened evaluation, transparency, security, risk assessment and incident management obligations.
- Fine-tuning or modifying a general-purpose AI model may, depending on the nature and extent of the modification, result in a new general-purpose AI model and may therefore trigger provider obligations for the entity carrying out that modification.
- The Code of Practice for general-purpose AI models published on 10 July 2025 helps general-purpose AI models providers identify specific technical and organisational measures to implement in order to comply with their obligations.
- Provisions regarding general-purpose AI models apply from 2 August 2025.

To do list

- [ ] Familiarise yourself with the concepts of general-purpose AI models, general-purpose AI systems, AI systems, and high-risk AI systems – and their relation to each other. This understanding is crucial for assessing which AI systems your company uses or markets and for making informed legal evaluations.
- [ ] Take a close look at the GPAI Guidelines published on 18 July 2025, as they – although not legally binding – provide valuable guidance in many areas, for example, on what exactly a general-purpose AI models is, what effects modifications may have, and under which circumstances a company is to be regarded as a provider of a general-purpose AI model, among other aspects.
- [ ] For providers of general-purpose AI models: undertake a thorough governance review and make necessary adjustments to ensure compliance.
- [ ] For providers of general-purpose AI models: conduct a comprehensive legal IP assessment – regulations for general-purpose AI models are heavily intertwined with IP laws, particularly regarding the copyright policy and the various training data obligations.
- [ ] For providers of general-purpose AI models: continuously and closely monitor the thresholds for *"systemic risk,"* as these may be adjusted over time via delegated acts.
- [ ] For providers of general-purpose AI models: review and consider whether to sign the Code of Practice for general-purpose AI models published on 10 July 2025. While the specific measures set out in the Code are not mandatory, the Commission has confirmed that the Code is an adequate voluntary tool for providers of general-purpose AI models to demonstrate compliance with the AI Act.

Background and relevance of general-purpose AI models

One of the most prominent debates in the legislative process of the AI Act revolved around the regulation of general-purpose AI. The first draft of the AI Act (the Commission's proposal of April 2021) was based on the understanding that each AI system is created for a specific purpose, and that this purpose can be associated with a specific risk potential. This classification did not have in mind foundation models which are trained on broad data such that they can be applied across a wide range of use cases. These AI models did not fit into the risk-based scheme of the first draft of the AI Act. The categorisation had to be expanded to include a new category that took into account the specific capabilities and dangers of such models. In the summer of 2023, the *"foundation model"* (later renamed general-purpose AI) was added to the then-current draft of the AI Act.

The AI Act's chapter on general-purpose AI models is of particular significance for two main reasons. First, it addresses AI models with broad, general-purpose capabilities, which include most current generative AI systems and underpin a large proportion of emerging business use cases. Secondly, the regulatory requirements applicable to general-purpose AI models—especially those posing systemic risk—sit alongside the high-risk AI regime, as the most demanding obligations to comply with under the AI Act, requiring a high level of technical, organisational and governance maturity from affected organisations.

While these obligations are formally directed at providers rather than deployers, they remain relevant across the AI value chain, as many AI systems will be built on general-purpose AI models.

Terminology and general-purpose AI value chain

General-purpose AI models and general-purpose AI systems

Article 3(63) outlines the characteristics of a general-purpose AI model, emphasising its versatility and competence across various tasks.

Recital 98 highlights two key indicators:

1. having at least a billion parameters; and

2. being trained with a large amount of data using self-supervision.

Such general-purpose AI models are distinguished by their ability to integrate into and function within diverse downstream systems or applications. Typically, general-purpose AI models undergo extensive training with large datasets, often utilising methods like self-supervision at scale. Recital 99 further specifies that large generative AI Models, such as LLMs or Diffusion Models, are typical examples of general-purpose AI models.

Recital 97 clarifies that while general-purpose AI models are crucial components of AI systems, they are not AI systems themselves. Additional elements, such as user interfaces, are needed to transform general-purpose AI models into fully operational AI systems. A general-purpose AI system is an AI system built upon a general-purpose AI model, maintaining its versatility across various tasks (article 3(66) and recital 100).

The GPAI Guidelines published on 18 July 2025 provide significantly greater clarity, beyond the relevant articles and recitals, regarding the categorisation of a general-purpose AI model. Specifically, the guidelines introduce two indicative criteria: a training compute threshold (10^{23} FLOPs) and the requirement of certain output modalities (language – text or audio – text-to-image, or text-to-video). If both criteria are met, the existence of a general-purpose AI model is presumed. However, it is important to note that despite these new criteria, the decisive factor remains whether the model genuinely has a general-purpose nature. In other words, there are cases in which both criteria may be fulfilled, yet the model would still not qualify as a general-purpose AI model – for example, where it serves only a narrow purpose. The GPAI Guidelines provide several examples of this, such

as AI models designed for transcribing speech to text, generating speech from text, or filling in damaged or missing parts of images.

General-purpose AI systems and high-risk AI systems

Recital 85 emphasises that general-purpose AI systems, due to their versatility, may function as high-risk AI systems or as components within them. Providers of general-purpose AI systems must collaborate closely with providers of high-risk AI systems to ensure compliance with the AI Act and to distribute responsibilities fairly along the AI value chain (see Chapter 4 for more on high-risk systems).

Modification and fine-tuning of general-purpose AI models

Modifying (for example, through fine-tuning) a general-purpose AI model, where a new specialised training data set is fed into the model to achieve better performance for specific tasks, does not transform it into a general-purpose AI system; it remains an abstract model without an interface – the change happens on the model level. Instead, such actions create a modified general-purpose AI model.

The GPAI Guidelines provide important clarification on when a modified model constitutes a new and independent general-purpose AI model. A key distinction is drawn based on who carries out the modification. Where the modification is performed by the original provider of the base model, it is considered to fall within the same AI lifecycle. In ˆthat case, the modification does not give rise to a new general-purpose AI model, and the original provider remains responsible under the existing provider obligations.

Where the modification is carried out by a third party, the assessment is more nuanced. According to the GPAI Guidelines, a downstream modifier becomes the provider of a new general-purpose AI model only where the modification results in a significant change in the model's generality, capabilities or systemic risk.

Training compute is used as an evidentiary indicator to support that assessment. The GPAI Guidelines state that an indicative criterion for determining when a downstream modifier should be considered the provider of a modified general-purpose AI model is that the training compute used for the modification exceeds one third of the training compute of the original model. Where this threshold is exceeded, this is indicative that a significant change in the model has occurred such that the downstream modifier should be considered a provider for that model; where it is not exceeded, this is indicative that the downstream modifier should not be considered a provider of the model.

The GPAI Guidelines further recognise that a downstream modifier may not know, and may not be able to reasonably estimate, the training compute of the original model. In such cases, the one-third comparison is replaced by the compute thresholds for when a model is considered a general-purpose AI model or general-purpose AI model with systemic risk. Where the original model is a general-purpose AI model with systemic risk, the relevant proxy is one third of the threshold for models presumed to have high-impact capabilities, currently set at 10^{25} FLOP under article 51(2). In all other cases, the proxy is one third of the threshold for models presumed to be general-purpose AI models, currently set at 10^{23} FLOP.

Recital 97 and recital 109 specify that the provider of a new general-purpose AI model that emerged through modification has limited obligations related only to the changes made, including providing technical documentation and the summary of the training data used for the modification.

Obligations for providers of general-purpose AI models

A provider of a general-purpose AI model that places such a model on the market, or integrates it with its own AI system and places it on the market or puts it into service, is obliged to:

a. prepare and maintain up-to-date technical documentation containing i.e. a description of the model and information on its development process (including training, testing and validation) for the purpose of making it available to the AI Office and competent authorities (article 53(1)(a)) – a list of the minimum information required is provided in Annex XI;

b. prepare, maintain up-to-date and make certain information and documentation

available to downstream AI systems providers (i.e. those who wish to integrate their AI systems with the general-purpose AI model) so that they can understand the model's characteristics and comply with their own obligations (article 53(1)(b)) – a list of the minimum information required is provided in Annex XII; providers are allowed to balance the information they share against their need to protect confidential business information and trade secrets;

c. establish a policy to comply with the EU regulations on copyright and related rights (article 53(1)(c)), and in particular, to identify and comply with reservations of rights made by rightsholders under article 4(3) ofDirective (EU) 2019/790 – on copyright and related rights in the Digital Single Market (the AI Act does not specify other matters that have to be addressed in the policy);

d. prepare and publicly share a comprehensive summary on the data used for training the model (article 53(1)(d)). The AI Office has published a template for this purpose, requiring general information on the provider, the model and its modalities; a list of data sources such as public databases, private databases, data crawled and scraped from online sources, user data, synthetic data, and other data; as well as data processing aspects, including compliance with the text and data mining exception;

e. cooperate with the relevant authorities when they exercise the powers granted to them under AI Act (article 53(3)); and

f. if the provider is established outside the EU: appoint an authorised representative in the EU (article 54(1)).

If a provider releases a general-purpose AI model under a free and open-source licence and makes relevant information publicly available, it is not obliged to fulfil the requirements listed in a-b and f above – unless the general-purpose AI model is qualified as presenting a systemic risk (article 53(2) and article 54(6)) for the modification.

General-purpose AI model providers who sign the Code of Practice for general-purpose AI models commit to demonstrating their compliance with transparency and copyright obligations by doing the following:

- Transparency
  - documenting and keeping up-to-date all the information outlined in the Model Documentation Form that forms part of the Code, e.g. model properties, methods of its distribution and relevant licenses, information on the model's acceptable uses, as well as on the model training process, including data, computational resources and energy used for that purpose.
  - disclosing contact information for the AI Office and downstream providers to request information and providing such information upon request and with no delay.
  - ensuring quality, integrity and security of the abovementioned information.
- Copyright
  - drawing up, keeping up-to-date and implementing a copyright policy that applies across all general-purpose AI models placed on the EU market and sets clear responsibilities for implementation and oversight.
  - where using web-crawling only extracting lawfully accessible content, without circumventing effective technical protection measures, and excluding domains listed on official piracy registers.
  - respecting machine-readable text- and data mining opt-out instructions (such as robots.txt) when employing web-crawlers and publishing crawler specifications.
  - implementing appropriate and proportionate technical safeguards to mitigate reproducing of training data in the outputs in an infringing manner and prohibiting copyright-infringing uses by users in the terms of use.
  - establishing a point of contact and an accessible complaint mechanism for rightsholders, with a clear contact point and fair, timely handling of substantiated claims.

General-purpose AI models with systemic risk

Qualification criteria

The AI Act introduces specific heightened obligations for general-purpose AI models presenting "systemic risks", e.g. reasonably foreseeable negative effects relating to major accidents, disruption of critical sectors, serious consequences to public health and safety, public and economic security, democratic processes, the dissemination of false or discriminatory content, etc. (recital 110).

According to article 51(1), a general-purpose AI model is classified as a general-purpose AI model with systemic risk if it meets one of these two conditions: (a) it has "high impact capabilities" evaluated on the basis of technical tools and methodologies, or (b) is designated by the Commission as having capabilities or impact equivalent to those set out in point (a) having regard to the criteria set out in Annex XIII. These criteria notably include the number of parameters of the model, the quality or size of the data set, the amount of computation used for training, the model's impact on the EU market, the number of registered users the EU.

A model is presumed to have *"high impact capabilities"* if it is trained with more than 10^{25} floating point operations, i.e., massive computing powers (article 51(2)). At the time of writing, only a handful of large language models seem to meet this threshold.

Article 52 sets out the classification procedure. Most notably, providers of general-purpose AI models which meet the systemic risk classification conditions must notify the Commission without delay, and at the latest within two weeks after that requirement is met or it becomes known that it will be met. Providers may present arguments to demonstrate that their models do not pose systemic risks despite meeting the requirements. Should such arguments be rejected by the Commission, the concerned models will be considered as presenting systemic isks. Upon "reasoned request" of a provider, the Commission may decide to reassess the classification (article 52(5)).

A list of general-purpose AI models with systemic risk will be published and updated by the Commission (article 52(6).

Obligations for providers of general-purpose AI models with systemic risk

In addition to the general requirements applicable to all general-purpose AI models providers, the AI Act imposes additional heightened obligations on providers of general-purpose AI models with systemic risk (article 55(1)). These obligations apply prior to the model's placing on the market and throughout their entire lifecycle, and relate to:

- model evaluation;
- assessment and mitigation of systemic risks;
- incident management and reporting;
- increased level of cybersecurity protection; and
- extended technical documentation.

The Safety and Security chapter of the Code of Practice for general-purpose AI models sets out voluntary measures which providers of general-purpose AI models with systemic risk can implement in order to demonstrate compliance with their enhanced obligations under the AI Act. These include concrete practices for managing systemic risks which notably include identifying, assessing and mitigating systemic risks and transparently reporting safety and security risks throughout the model's lifecycle and developing cybersecurity measures.

The Safety and Security chapter of the Code of Practice provides ten detailed obligations which signatories of the Code of Practice commit to:

- **Commitment 1:** Adopting a state-of-the-art safety and security framework, prior to model deployment, to outline systemic risk management processes and measures ensuring systemic risks from general-purpose AI models are acceptable. The framework must contain a high-level description of implemented and planned processes and measures for systemic risk assessment and mitigation. Signatories must define assessment criteria, risk classifications, mitigation approaches, predictive methodologies, and organisational responsibilities. This framework should be implemented and regularly updated in response to new risks, incidents, or significant changes in the model or its environment.

- **Commitment 2:** Identifying systemic risks stemming from the model to facilitate systemic risk analysis and acceptance determination. This includes following a structured identification process (e.g., compiling a list of risks that could stem from the model and be systemic and identify their nature and sources) and developing risk scenarios (commitment 2). Appendix 1.4 to the Code of Practice identifies four specified systemic risks (in addition to the broader identification process): (i) the enablement of chemical, biological, radiological or nuclear harm; (ii) the loss of effective human control over AI systems; (iii) the facilitation of large-scale cyber-attacks, including against critical infrastructure; and (iv) the manipulation of human behaviour or decision-making at scale through targeted persuasion or deception.

- **Commitment 3:** Analysing each identified systemic risk to facilitate systemic risk acceptance determination. This involves five elements: i) gathering model-independent information (e.g., web searches, literature reviews, market analysis, expert interviews), ii) conducting model evaluations, iii) modelling the systemic risk, iv) estimating the systemic risk, and v) conducting post-market monitoring ncluding through end-user feedback, incident reporting, bug bounties, and community evaluations.

- **Commitment 4:** Specifying systemic risk acceptance criteria, determining if risks are acceptable, and deciding whether to proceed with development, market availability, and/or use based on this determination. Signatories may only proceed if systemic risks are determined acceptable. This includes describing and justifying, in the framework established under Commitment 1, how they will determine whether the systemic risks stemming from the model are acceptable, applying defined risk-tier frameworks with built-in safety margins. If risks are deemed unacceptable, immediate corrective actions are required.

- **Commitment 5:** Implementing appropriate safety mitigations throughout the model lifecycle to ensure systemic risks remain acceptable. Safety mitigations must be appropriate and sufficiently robust under adversarial pressure including (i) filtering and cleaning training data, (ii) monitoring and filtering the model's inputs and/or outputs, (iii) changing the model behaviour in the interests of safety, such as fine-tuning the model to refuse certain requests or provide unhelpful responses and (iv) staging the access to the model, e.g. by limiting API access to vetted users, gradually expanding access based on post-market monitoring, and/or not making the model parameters publicly available for download initially.

- **Commitment 6:** Implementing adequate cybersecurity protection for the providers' models and physical infrastructure throughout the model's lifecycle to ensure risks from unauthorised releases, access, and theft remain acceptable. This includes defining security goals and implementing appropriate security measures. A model is exempt from this commitment if the model's capabilities are inferior to the capabilities of at least one model for which the parameters are publicly available for download.

- **Commitment 7:** Reporting to the AI Office information about the model and the provider's systemic risk assessment and mitigation processes by preparing a safety and security model report before placing a model on the market. Reports include model descriptions and behaviour, justifications for proceeding, documentation of risk processes, external reports, and information about material changes to the risk landscape. Signatories commit to updating their model report if they have reasonable grounds to believe that the justification for why the systemic risks stemming from the model are acceptable has been materially undermined.

- **Commitment 8:** Defining clear responsibilities for managing systemic risks across all organisational levels. Signatories must clearly assign oversight, ownership, monitoring, and assurance roles within their governance structures and ensure adequate resources, a strong risk culture, and protections for whistleblowers.

- **Commitment 9:** Implementing processes for tracking, documenting, and reporting serious incidents to the AI Office and national authorities according to severity and tight deadlines (for example, within two days for incidents affecting critical infrastructure). Reports must be regularly updated and kept for at least five years.

- **Commitment 10:** Documenting implementation of the Safety and Security chapter of the Code of Practice. Signatories must draw up and maintain up-to-date additional information and provide it to the AI Office upon request (e.g., description of the model's architecture, description of how the model is integrated into AI systems). Signatories are required to retain detailed records of their documentation and safety and risk management activities for a minimum of ten years. In addition, they must publish (e.g., on their websites) summarised versions of the framework and model reports, where needed to reduce risks, unless the model meets specific criteria qualifying it as "*similarly safe or safer*".

Transparency

At a glance

In addition to specific transparency requirements for high-risk AI systems (see Chapter 4), the AI Act mandates freestanding transparency requirements under article 50 for specific types of AI systems, requiring that adequate information be provided to individuals, by either providers or deployers.

- **Direct AI Interaction:** providers of AI systems intended to interact directly with individuals need to design and develop them, so that the individuals will be informed about the fact that they are interacting with an AI system.
- **Synthetic media marking:** providers of AI systems must mark AI-generated content (audio, images, videos, text) in a machine-readable format and ensure it is detectable as artificially generated or manipulated.
- **Deepfake labelling:** deployers of AI systems that generate or manipulate content (images, audio, video) constituting a deepfake, as well as text published for the purpose of informing the public on matters of public interest, must disclose that the content has been artificially generated or manipulated.
- **Emotion recognition system/biometric categorisation system:** deployers of these AI systems must make individuals exposed to them aware of their operation.

The AI Act's transparency obligations collate with other regulatory frameworks in the EU. In particular, there is some overlap between the transparency requirements of the GDPR and the AI Act, although the latter is more technical in nature.

To do list

- [ ] Look out for publication on the Commission's guidelines on article 50 transparency obligations and the Code of Practice for Transparency of AI-Generated Content (which will provide voluntary measures to demonstrate compliance with articles 50(2) and 50(4)) during 2026.

For providers

- [ ] **Implement synthetic media marking:** identify and implement technical solutions to ensure content generated or manipulated by the AI system is marked in a machine-readable format.
- [ ] **Review whether direct AI interaction notifications are required:** consider whether it will be obvious to users that they are directly interacting with an AI system and add notifications where this may not be obvious.

For deployers

- [ ] **Deepfake labelling:** label deepfakes (and text published for the purpose of informing the public on matters of public interest) in a clear and distinguishable manner to disclose their artificial creation or manipulation.
- [ ] **Emotion recognition system/ biometric categorisation system:** make individuals exposed to these systems aware of their operation.

General transparency obligations

The AI Act acknowledges the importance of transparency in the use of AI systems. Individuals should be enabled to understand the AI system's design and use, and there should be accountability for decisions made by companies and public authorities. Transparency is also essential for creating public trust in AI systems and ensuring their responsible deployment.

Transparency also enhances the broader concept of 'AI literacy', developing awareness about the opportunities and risks of AI and the possible harm it can cause. Such awareness should especially be developed amongst:

- individuals concerned, giving them a better understanding of their rights in the context of AI, and
- deployers, allowing them to deploy AI systems in an informed way.

Providers, and in certain circumstances deployers as well, have their own transparency requirements.

The transparency requirements for specific types of AI systems are described below. These obligations apply in addition to the transparency obligations imposed on high-risk systems (e.g. on providers under article 13 and deployers of Annex III high-risk systems under article 26(11)) and other transparency obligations imposed under EU or national law (article 50(6)).

Provider Obligations

Direct AI interaction notification (article 50(1))

Article 50(1) requires providers to ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the individuals concerned are informed that they are interacting with an AI system. This requirement may be satisfied either through an express notification or where, taking into account the circumstances and context of use, it is obvious to a reasonably well-informed, observant and circumspect person that the interaction is with an AI system. A common example where this obligation is relevant is the provision of chatbot-based customer support systems, which should be designed so that users are made aware that the interaction is with an AI system rather than a human.

- **Implementation:** The AI Act does not prescribe a specific technical form or format for informing individuals that they are interacting with an AI system. However, the information must be provided in a clear and distinguishable manner, at the latest at the time of the first interaction or exposure, and must comply with applicable accessibility requirements, e.g. under Directive 2019/882 (article 50(6)).
- **Exemption for law-enforcement use:** The transparency requirement in Article 50(1) does not apply to AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences, provided that appropriate safeguards for the rights and freedoms of third parties are in place. This carve-out does not apply where such systems are made available for the public to report criminal offences.

Marking of AI-generated and manipulated content (article 50(2))

Article 50(2) mandates that providers of AI systems, including general-purpose AI systems, must appropriately mark synthetic audio, image, video, or text content. Recital 133 explains the rationale: with AI technology advancing, AI-generated synthetic content is becoming increasingly indistinguishable from human-generated content, posing the risk of misinformation, manipulation, fraud, impersonation, and consumer deception.

The obligation imposed by article 50(2) applies to the provider of the AI system, and not to the provider of any general-purpose AI model which may form part of that AI system (although in some cases, the model provider and AI system provider will be the same entity). In practice, downstream providers of AI systems based on general-purpose AI models may nevertheless require technical support from model providers to enable compliance with the marking requirement.

Nature of the marking obligation

Article 50(2) does not prescribe specific technical solutions for marking AI-generated or manipulated content. Instead, it establishes a principle-based obligation requiring that:

- the marking be provided in a machine–readable format indicating that the content is artificially generated or manipulated;
- the context is detectable as artificially generated or manipulated; and
- the technical solutions adopted are effective, interoperable, robust and reliable, taking into account the type of content, the state of the art, implementation costs, and available technical standards.

Beyond these general parameters, the AI Act leaves flexibility as to the specific technical means used to implement marking, anticipating that further detail will be provided through harmonised standards, technical specifications and guidance developed over time. This includes the development of Commission guidelines on transparent AI systems and the Code of Practice on marking and labelling of AI-generated content — including the first draft published in December 2025 and further drafts anticipated in 2026 — as they are expected to offer practical guidance on how to meet the article 50(2) transparency and marking obligations.

Article 50(5) requires that "*the information*" referred to by article 50(2) shall be provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure and shall conform to the applicable accessibility requirements. It is not clear from article 50(5) whether "*the information*" refers to the marking, the detection of the content as artificially generated or manipulated, or both. While not determinative, the first draft of the Code of Practice suggest it applies to the detection of the content and includes a measure that AI system providers who sign the Code of Practice will commit to providing an interface (e.g. API or user interface) or a publicly available detector to enable users and other interested parties to verify with confidence scores whether content has been generated or manipulated by their AI system or model.

Exemptions

- **Editorial assistance:** The marking obligation does not apply to the extent the AI system performs an assistive function for standard editing or does not significantly change the original input data. The scope of this exception is expected to be addressed in the forthcoming Commission guidelines.
- **Legal use:** AI systems that are authorised for use in detecting, preventing, investigating, or prosecuting criminal activities are also exempt from the marking requirement.

Deployer obligations

Emotion recognition/biometric categorisation systems (article 50(3))

Article 50(3) imposes specific transparency obligations for deployers of:

- **Emotion recognition systems:** AI systems used for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data, such as facial expressions, voice characteristics or other physiological signals.

or

- **Biometric categorisation systems:** AI systems used for the purpose of assigning natural persons to specific categories on the basis of their biometric data, for example categories relating to physical characteristics such as sex, age range, hair colour, eye colour or visible marks such as tattoos.

Further details on the contexts in which the use of emotion recognition or biometric categorisation systems is prohibited are set out in Chapter 3 of this guide, and on when such systems are classified as high-risk AI systems in Chapter 4.

Where the use of such an AI system does not constitute a prohibited practice, and in addition to any obligations applicable to deployers of high-risk AI systems (e.g. article 26(11)), deployers must inform the natural persons concerned that they are subject to the use of an emotion recognition or biometric categorisation system. In particular, individuals must be informed when they are exposed to AI systems that process their biometric data in order to identify or infer

emotions or intentions or to assign them to biometric categories. This information must be provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure and conform to the applicable accessibility requirements (article 50(5)).

Exemptions

- **Legal use:** AI systems that are permitted for use in detecting, preventing or investigating criminal activities that are subject to appropriate safeguards for the rights and freedoms of third parties and in accordance with the EU law, are exempt from these requirements.

- **Ancillary biometric categorisation:** Recital 16 and article 3(40) clarify that biometric categorisation systems do not include features that are purely ancillary to another commercial service, where the feature is strictly necessary for objective technical reasons, cannot be used independently of the main service, and is not designed or used as a means of circumventing the AI Act. The Commission's guidelines on Prohibited Practices further explain that such ancillary features fall outside the scope of biometric categorisation systems only where their functionality is inseparable from the primary service and does not enable biometric categorisation as an autonomous or standalone use case.

Interaction with Data Protection Law

Deployers, when using these AI systems, process personal data in accordance with GDPR and (EU) 2018/1725 and Directive (EU) 2016/680, as applicable, apart from the requirements on the legal basis of the processing. This means that these regulations also constitute separate transparency obligations for deployers acting as controllers. In such cases, individuals should nevertheless be informed about the processing of their data as required under article 13 and 14 GDPR. In relation to any automated processing, controllers are expected to additionally explain the logic behind their decision-making. In the case of an AI system, this might be provided as part of an explainability statement – a document providing a non-technical explanation of i.e. why the organisation uses AI, how AI was developed, and how it operates and is used.

Deepfakes and text informing the public on matters of public interest (article 50(4))

Article 50(4) imposes specific labelling obligation for (i) deployers of AI systems regarding AI generated or manipulated content known as "*deepfakes*"; and (ii) deployers AI systems that generates or manipulates text which is published with the purpose of informing the public on matters of public interest.

These obligations apply to the deployer of the AI system, rather than its provider. However, AI system providers are likely to be encouraged (e.g. via the relevant Code of Practice) to incorporate functionality into their AI systems which allows deployers to apply a label to the content they generate using that system.

Definition of deepfakes (article 3(60))

The obligation applies to deployers who use an AI system to generate or manipulate images, audio, or video content that:

- significantly resembles real people, objects, places, entities, or events; and

- could mislead a person into believing the content is authentic or truthful.

Examples of deepfakes could include:

- AI-generated audio of a politician misleading voters about election dates.

- AI-manipulated videos showing a specific branded consumer product (e.g. a particular model of a smartphone or vehicle) malfunctioning or exploding, falsely suggesting real defect.

- AI-generated footage purporting to show a real, identifiable location (such as an airport, train station or public square) in a state of emergency, evacuation or disorder that never took place.

- Synthetic news clips falsely showing that a real-world incident (for example, a plane crash, terrorist attack or natural disaster) has taken place when it has not.

Nature of the labelling and disclosure obligation for deepfakes

The AI Act does not prescribe specific technical solutions or visual formats for disclosing that content has been generated or manipulated by an AI system. Instead, the transparency obligations in article 50(5) establish a principle-based requirement that, where applicable, the disclosure must:

- be provided in a clear and distinguishable manner;
- be made at the latest at the time of the first interaction or exposure; and
- comply with applicable accessibility requirements.

Further practical detail on acceptable disclosure approaches is expected to be developed through Commission guidelines on transparent AI systems and the Code of Practice on marking and labelling of AI-generated content, including the first draft published in December 2025 and further drafts anticipated in 2026, which are intended to support implementation of the transparency obligation under Article 50(4).

Exemptions to deepfake labelling requirements

Article 50(4) provides the following exceptions to the deepfake labelling requirements:

- The transparency requirements are more relaxed for artistic, creative, satirical, fictional, or similar works. Examples of such works include AI-generated movies or parodies, digital art exhibits, and AI-generated music videos. In these instances, the obligation is to disclose the AI involvement in a manner that does not disrupt the viewer's experience. This can be achieved through subtle watermarks, brief audio disclaimers, or notes in the description texts on digital platforms.
- The obligation to label AI-generated content does not apply if the AI system's use is legally authorised for the purposes of detecting, preventing, investigating or prosecuting criminal offences.

AI-generated text published on matters of public interest (article 50(4))

In addition to its deepfake labelling obligations, Article 50(4) also introduces a specific transparency obligation for deployers of AI systems that generate or manipulate text which is published for the purpose of informing the public on matters of public interest. In such cases, deployers must disclose that the text has been artificially generated or manipulated, ensuring transparency in contexts where public trust and democratic discourse are particularly sensitive.

This disclosure obligation does not apply where the use of the AI system is authorised by law for the detection, prevention, investigation or prosecution of criminal offences. It also does not apply where the AI-generated text has undergone human review or editorial control, and where a natural or legal person assumes editorial responsibility for the publication of the content. This reflects the AI Act's recognition of existing editorial accountability frameworks, particularly in journalistic and media contexts.

Transparency obligations for high-risk AI systems

Article 50(6) explains that the transparency obligations outlined here operate alongside other regulatory requirements. They neither replace nor reduce the obligations specified in Chapter III or other transparency requirements under EU or EU Member State legislation.

See Chapter 4 of this guide for more details.

Transparency obligations at the national level and codes of practice

The transparency obligations outlined in article 50(1)-(4) are designed to coexist with other regulatory requirements, according to article 50(6). They neither replace nor diminish the requirements set forth in Chapter III or other transparency mandates under EU or national law.

The AI Office is responsible for promoting and facilitating the development of Codes of Practice to support the effective implementation of the transparency obligations under article 50(1)-(4) at the EU level, under article 50(7). These codes are intended to clarify the methods for detecting and labelling AI-generated content, to enhance cooperation throughout the value chain, and to ensure that the public can clearly distinguish between content created by humans, and content generated by AI (recital 135).

Relationship with other regulatory frameworks

- The AI Act's marking obligations under article 50(2) and (4) are intended to support the Digital Services Act's (DSA) requirements for very large online platforms (VLOP) and search engines (VLOS) to identify and mitigate the risks associated with the dissemination of deepfakes (article 33 et seq. DSA). If the AI provider is separate from the VLOP or VLOS, these markings enable the platforms to recognise AI-generated content more efficiently. Conversely, if a VLOP or VLOS is also the AI provider, their DSA obligations are further detailed and enhanced by the AI Act.

- The transparency regulations for deepfakes will correlate with the European guidelines on misleading advertising (e.g. the Unfair Commercial Practices Directive) as well as national criminal provisions on deepfakes.

- The AI Act's transparency obligations also support and supplement the transparency requirements under Regulation (EU) 2016/679. However, the GDPR transparency requirements apply if personal data is processed when using AI technologies at all different stages of the AI lifecycle (e.g. when developing, testing or deploying AI technologies), and apply to controllers. Developers and providers of AI tools will not always be acting in such a role. In such case they may still be obliged to provide specific information to controllers to enable the latter to meet their obligations.

AI regulatory sandboxes

At a glance

- The AI Act enables the establishment of *"AI regulatory sandboxes"* to provide a controlled environment in which to test innovative AI systems for a limited period before they are placed on the market.
- This regime is intended to encourage AI providers (or potential providers) to experiment with new and innovative products under supervision by regulators. There are specific incentives aimed at encouraging participation by SMEs and start-ups.
- Each EU Member State must establish at least one AI regulatory sandbox by 2 August 2026, although this can be done in co-operation with other EU Member States.
- The Commission is expected to adopt implementing acts to set out detailed arrangements for the establishment, operation and supervision of AI regulatory sandboxes.
- The AI Act also provides for *"real-world"* testing of AI systems, both inside and outside of regulatory sandboxes, subject to certain conditions to protect participants.
- The regimes relating to AI regulatory sandboxes and real-world testing are intended to be harmonise across the EU. However, there is the potential for divergent approaches at a national level, leading to a possibility of *"forum shopping"* by providers.

To do list

- [ ] Participation in AI regulatory sandboxes and real-world testing is voluntary. AI providers should familiarise themselves with the relevant provisions of the AI Act if they intend to participate in a sandbox or real-world tests and should look out for further announcements and guidance on these topics, including detailed arrangements for AI regulatory sandboxes to be specified by the Commission in due course.
- [ ] You should think about the countries in which you would like to test your AI services/products. Although the AI Act intends to establish a harmonised regime, there may be national differences which make some EU Member States more appropriate for you than others.
- [ ] Once you decide to participate in an AI regulatory sandbox, you will need to prepare a sandbox plan and follow the guidelines and supervision provided by the relevant national competent authority. If you decide to conduct real-world tests, you will also need to prepare a testing plan and seek approval from the relevant market surveillance authority.
- [ ] When you successfully complete an AI regulatory sandbox process, you should obtain an exit report from the relevant national competent authority. This may be useful to accelerate the conformity assessment process for your AI product/service.

AI regulatory sandboxes

The AI Act enables the creation of *"regulatory sandboxes"* to provide a controlled environment in which to test innovative AI systems for a limited period before they are placed on the market or otherwise put into service. The objectives of the AI regulatory sandbox regime include:

- fostering AI innovation while ensuring innovative AI systems comply with the AI Act;
- enhancing legal certainty for innovators;
- enhancing national competent authority understanding of the opportunities, risks and the impacts of AI use;
- supporting cooperation and the sharing of best practices; and
- accelerating access to markets, including by removing barriers for SMEs and start-ups.

What is a regulatory sandbox under the AI Act?

The AI Act defines an *"AI regulatory sandbox"* as:

"*a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision.*"

AI regulatory sandboxes can be established in physical, digital or hybrid form and may accommodate physical as well as digital products.

Obligation on EU Member States to establish AI regulatory sandboxes

The obligation to establish AI regulatory sandboxes rests with the EU Member States and their national competent authorities (see Chapter 8 for more on these). Each EU Member State must establish at least one AI regulatory sandbox by 2 August 2026. However, EU Member States can choose to either (i) establish one or more AI regulatory sandboxes at national level; (ii) jointly establish a sandbox with the national competent authorities of one or more other EU Member States or (iii) participate in an existing sandbox.

National competent authorities establishing AI regulatory sandboxes should cooperate with other relevant national competent authorities where appropriate and may also involve other actors within the AI ecosystem. The EU Data Protection Supervisor may also establish an AI regulatory sandbox for EU institutions, bodies, offices and agencies.

A list of planned and existing sandboxes will be made publicly available by the AI Office. The Commission also intends to develop a single interface containing relevant information relating to AI regulatory sandboxes to allow stakeholders to:

- interact with AI regulatory sandboxes;
- raise enquiries with national competent authorities; and
- seek non-binding guidance on the conformity of innovative AI products, services or business models.

Who can participate in AI regulatory sandboxes?

The sandbox regime is aimed at providers (or prospective providers) of AI systems, although applications can be submitted in partnership with deployers and other relevant third parties.

There are specific provisions which are designed to encourage participation by SMEs and start-ups, including:

- access to sandboxes should generally be free of charge for SMEs and start-ups;
- priority access for SMEs and start-ups with a registered office or branch in the EU; and
- SMEs and start-ups should have access to guidance on the implementation of the AI Act and other value-added services.

Liability

Administrative fines under the AI Act will not be imposed on prospective providers if:

- they observe the relevant sandbox plan and the terms and conditions for their participation; and
- follow (in good faith) any guidance given by the national competent authority.

However, providers and prospective providers participating in an AI regulatory sandbox (including SMEs and start-ups) will remain liable for any harm caused to third parties as a result of the experimentation taking place in the sandbox and they will not be exempt from criminal liability or from enforcement under other applicable EU or national laws.

Implementation of the sandbox regime

In order to avoid fragmentation across the EU, the Commission intends to adopt implementing acts specifying the detailed arrangements for the establishment, operation and supervision of AI regulatory sandboxes, including common principles on:

- eligibility and selection criteria for participation;
- procedures for the application, participation, monitoring, exiting from and termination of sandboxes; and
- the terms and conditions applicable to participants.

These implementing acts are intended to ensure that AI regulatory sandboxes:

- are open to any provider who meets fair and transparent eligibility criteria;
- allow broad and equal access and keep up with demand for participation;
- facilitate the development of tools and infrastructure for testing and explaining dimensions of AI systems relevant for regulatory learning, such as accuracy, robustness and cybersecurity, as well as measures to mitigate risks to fundamental rights and society at large;
- facilitate the involvement of relevant actors within the AI ecosystem (e.g. notified bodies and standardisation organisations, testing and experimentation facilities, research and experimentation labs and European Digital Innovation Hubs), and also that participation in an AI regulatory sandbox is uniformly recognised (and carries the same legal effects) across the EU.

National competent authority obligations

National competent authorities must:

- allocate sufficient resources to ensure their sandbox regime complies with the requirements of the AI Act;
- provide guidance to sandbox participants on how to fulfil the requirements of the AI Act;
- provide participants with an exit report detailing the activities carried out in the sandbox, results and learning outcomes, and while an exit report does not constitute a conformity assessment or presumption of compliance, it may be taken into account by notified bodies or market surveillance authorities when assessing conformity;
- provide annual reports to the AI Office and the Board (see Chapter 8 for more on these), identifying best practices, incidents and lessons learnt.

National competent authorities will retain supervisory powers in relation to sandbox activities, including the ability to suspend or terminate activities carried out within a sandbox where it is necessary to address significant risks to fundamental rights or health and safety.

Processing of personal data within sandboxes

Personal data which has been lawfully collected for other purposes can be used in an AI regulatory sandbox subject to compliance with various conditions set out in the AI Act (all of which must be met for the relevant processing activities to be permitted). Some of the key conditions include:

- the relevant AI system being deployed in the sandbox must be aimed at safeguarding substantial public interest (e.g. public health, energy sustainability, safety of critical infrastructure);

- use of the personal data must be necessary and could not be substituted with anonymised or synthetic data;
- the personal data must be handled in a separate and protected environment and must be subject to appropriate technical and organisational measures; and
- a detailed description of the process and rationale behind the training, testing and validation of the AI system is retained, together with the testing results.

Real-world testing of AI systems

The AI Act also enables the testing of AI systems in "real-world conditions", subject to certain conditions.

> The AI Act defines *"testing in real-world conditions"* as follows:
>
> *"the temporary testing of an AI system for its intended purpose in real-world conditions outside a laboratory or otherwise simulated environment, with a view to gathering reliable and robust data and to assessing and verifying the conformity of the AI system with the requirements of [the AI Act]*".

Such real-world testing will not qualify as placing the relevant AI system on the market or putting it into service, provided that the relevant requirements of the AI Act are complied with. (See Chapter 2 for more on these concepts).

The AI Act primarily focusses on real-world testing of high-risk AI systems outside of AI regulatory sandboxes. However, the AI Act also contemplates the possibility of AI systems (whether high-risk or not) being subject to real-world testing within the framework of an AI regulatory sandbox, under the supervision of a national competent authority.

In both scenarios, the real-world testing must comply with various conditions set out in the AI Act (all of which must be met for the testing to be permitted, although there is greater flexibility where the testing is conducted within a sandbox). Some of the key conditions include:

- the proposed real-word tests have been approved by the relevant market surveillance authority and registered in the EU database for high-risk AI systems;
- the provider conducting the testing is established in the EU (or has appointed a legal representative established in the EU);
- testing is limited to a maximum of 6 months (which can be extended for an additional 6 months, although this requirement can be derogated from in relation to real-world testing within a sandbox environment);
- participants in the real-world testing are properly protected – they must give informed consent, outcomes must be reversible (or capable of being disregarded) and they must be able to withdraw at any time; and
- market surveillance authorities can conduct unannounced inspections on the conduct of real-world tests.

Providers and prospective providers will be liable for any damage caused in the course of their real-world testing.

Is there a risk of *"forum shopping"* in relation to participation in sandboxes and real-world testing?

Although the AI Act aims to harmonise the regimes relating to AI regulatory sandboxes and real-world testing across the EU, industry representatives and stakeholders will no doubt closely monitor their development and may elect participate in sandboxes and/or real-world testing in jurisdictions which are perceived to have the most industry-friendly approach (including in how liability relating to participation in sandboxes or real-world testing is determined).

Enforcement and governance

At a glance

- The AI Act puts in place a post-market monitoring, reporting and information sharing process.
- There are multiple reporting obligations:
  - By deployers to providers in line with the post-market monitoring plan.
  - By all operators, to providers/market surveillance authorities if a high-risk AI system presents a risk to health, safety or fundamental rights.
- By providers and deployers to market surveillance authorities in the event of a serious incident.
- Reports need to be made to market surveillance authorities in EU Member States where the incident occurred; reporting to multiple authorities may therefore be needed.
- There is a multi-pronged approach to enforcement:
  - The European Data Protection Supervisor handles EU institutions etc.
  - The Commission handles providers of general-purpose AI models.
  - Competent authorities in each EU Member State are otherwise responsible.
- Sanctions are tiered, by reference to the seriousness of the provision that has been infringed.
- Affected persons have a right to explanation of individual decision-making.

To do list

Providers of high-risk AI systems should:

- Watch for the Commission template post-market monitoring plan.
- Prepare and implement a post-market monitoring plan.
- If already subject to existing post-market monitoring obligations, or a regulated financial services provider, consider if you can integrate your AI Act obligations into these systems.

Providers of high-risk systems should:

- Consider if they are already subject to other equivalent obligations; if so, check if you have double reporting obligations or not.
- Ensure quality management systems include serious incident reporting procedures.
- Ensure these procedures establish the nature of the serious incident (death, serious harm to health, violation of fundamental rights etc) and if they are widespread.
- Identify to whom you would have to report.

Deployers of high-risk systems should:

- Check providers required reporting.
- Develop reporting plans to providers and market surveillance authorities for AI system risks and serious incidents.

Overview

The AI Act outlines a governance framework that provides for the implementation and supervision of both the ex ante requirements for AI systems and ex post surveillance and enforcement. The former is described in preceding chapters. The latter is the subject of this chapter, together with a description of the governance structure.

The enforcement regime addresses two types of risk: risks to product safety, and risks to fundamental rights. In relation to the former, the AI Act builds upon existing product safety legislation and is mostly enforced by national market surveillance authorities. Where risks to fundamental rights are identified, the market surveillance authorities shall inform and fully cooperate with the relevant national public authorities or bodies protecting fundamental rights.

Consistent with the risk-based approach in the AI Act, a multi-layered enforcement structure with different regimes applying to AI systems with varying risks is provided. For high-risk AI systems, the AI Act mandates, firstly, post-market monitoring applicable to all operators and reporting of serious incidents. The serious incident reporting obligations also apply to deployers, who should therefore also be aware of them.

The market surveillance authorities can require operators to take all appropriate measures to ensure that AI systems do not present a risk and, where necessary, can demand the withdrawal of a product or AI system from the market. Very significant fines for non-compliance with the terms of the AI Act can also be levied.

For general-purpose AI models, the Commission has exclusive powers to supervise and enforce the obligations in the AI Act.

The governance structure in the AI Act provides for the setting up of new institutional bodies at both the EU level (the AI Office, the Board, the Advisory Forum and the Scientific Panel) and national level (notifying authorities and market surveillance authorities) and the roles and competencies of each of them are outlined. The coordination between these bodies will be key to the effective implementation and enforcement of the AI Act.

Topics addressed in this chapter are as follows:

- Post-marketing obligations
- Market surveillance authorities
- Procedures for enforcement
- Authorities protecting fundamental rights
- General-purpose AI models
- Penalties
- Remedies for third parties
- Governance

Post-marketing obligations

Post-market monitoring system for high-risk AI systems

Since AI systems have the ability to adapt and continue to learn after they are placed on the market, it is important to monitor their performance once they are put on the market. Recital 155 explains that the aim of the post-market monitoring system is to ensure that providers of high-risk AI systems can consider experience from use of the system, so as to ensure ongoing compliance and improvement of the system.

All operators have obligations regarding post market monitoring, where an AI system presents a risk to health, safety or fundamental rights. Providers must report such risks immediately to market surveillance authorities (article 20). Deployers must report to providers, distributors and market surveillance authorities – and must suspend use of the system. Distributors and importers must also notify the market surveillance authorities.

"*Product presenting a risk*" means a product with the potential to affect adversely health and safety of persons in general, health and safety in the workplace, protection of consumers, the environment, public security or other public interests, protected by the applicable EU harmonisation legislation, 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 of the product , including its duration of use and, where applicable, its putting into service, installation and maintenance requirements.

Providers of high-risk AI systems must include a post-market monitoring plan as part of the technical documentation that they draw up before they put the system on the market (articles 72(3) and 11(1)). This plan must be in line with the Commission template. The post-marketing obligations will ensure that any need to immediately apply any necessary corrective or preventative actions are identified (article 3(25)).

Article 72 provides that the post-market monitoring system (and the documentation of the system) must be proportionate to the nature of the AI technology and the risks of the systems. This system must actively and systematically collect, document, and analyse relevant data throughout the AI system's lifetime, so as to allow the provider to evaluate continuous compliance. The data could be provided by deployers, or by others (although sensitive operational data from deployers who are law-enforcement authorities is excluded). Where relevant, the system should also include analysis of interactions with other AI systems, including devices and software.

Providers of certain types of high-risk AI systems, who already have post-market monitoring systems in place, can integrate their obligations under the AI Act into those existing systems, provided this achieves an equivalent level of protection. This is the case for high-risk AI systems covered by EU harmonisation legislation listed in Section A of Annex I (i.e. including certain machinery, toys and medical devices). It's also the case for financial institutions who are subject to requirements under EU financial services law regarding their internal governance, arrangements or processes, where these institutions place on the market high-risk AI systems listed in Annex III point 5 (in particular, evaluation of creditworthiness or for risk assessment and pricing in relation to life and health insurance) (article 72(4)).

Reporting of information on serious incidents for high-risk AI systems

Providers of high-risk AI systems must report "*serious incidents*" and the provider's quality management system must contain procedures relating to this (article 17(1)(i)).

Serious incidents are defined at article 3(49) and mean an incident or malfunctioning of an AI system that directly or indirectly causes:

- death, or serious harm to a person's health;
- serious and irreversible disruption to management or operation of critical infrastructure;
- violation of EU laws protecting fundamental rights; or
- serious harm to property or the environment.

Deployers must report serious incidents immediately first to providers and importers or distributors and then to market surveillance authorities. For providers serious incidents must be reported within set timelines, as set out below. If necessary, the provider or deployer may submit an initial report, which can be completed later (article 73(5)).

Situation	Period
Widespread infringement Or Serious incident involving critical infrastructure	Immediately ≤ than 2 days after awareness of the incident
Death of a person	≤ 10 days after awareness of the serious incident; or Immediately after establishing or suspecting a causal relationship between the serious incident and the AI system if earlier
Other situations (i.e. serious harm to health, fundamental rights violations, serious harm to property or environment – unless these are widespread)	≤ 15 days after awareness of the serious incident; or Immediately after the provider has established a causal link, or the reasonable likelihood of a link, between the AI system and the serious incident

If a deployer cannot reach a provider, then the obligation to consider reports when there is awareness or suspicion of a causal link with the serious incident, within the relevant deadlines, falls on the deployer. After reporting, the provider must promptly conduct necessary investigations, including a risk assessment and corrective actions. The provider must not do anything that would alter the AI system in a way that may affect any subsequent evaluation of the cause of the incident before it has informed the competent authorities.

Reports of serious incidents have to be made to the market surveillance authorities of the EU Member States where the incident occurred (article 73(1)). It follows that if a serious incident affects multiple EU Member States or affects multiple sectors so that there are multiple market surveillance authorities within an EU Member State, then multiple reports will need to be made.

The market surveillance authority must take appropriate measures (which can include withdrawal or recall of the product) within seven days of receiving the notification and must also immediately notify the Commission of any serious incident, whether or not they have taken action (article 73(8/11)).

Draft Guidance on high-risk systems incident reporting was published by the Commission (along with a draft reporting template) for consultation in September 2025. Final versions are expected to be published during the course of 2026.

Non-high-risk AI systems

AI systems relating to products that are not high-risk nevertheless must be safe when placed on the market or put into service. Regulation (EU) 2023/988 on general product safety and Regulation (EU) 2019/1020 on market surveillance and compliance of products apply to all AI systems governed by the AI Act, but these two Regulations provide the safety net for nonhigh-risk products (recital 166 and article 74(1)).

Regulation (EU) 2019/1020 requires all operators to inform the relevant market surveillance authority when they have reason to believe that a product presents a risk under article 3(19) (see definition below). To the list of risks in article 3(19), the AI Act has added risks to fundamental rights of persons (article 79(1)).

Market surveillance authorities

EU Member States play a key role as the enforcement of the AI Act will often require a local presence. EU Member States must each designate at least one market surveillance authority and one, if there is more than one, of these authorities must be set as a single point of contact vis-à-vis the public and other counterparts at EU Member State and EU level. The EU Member State shall notify the Commission of the single point of contact and the Commission will make a list of them available to the public (recital 153 and article 70(1/2)). The EU Member States had until 2 August 2025 to comply with these provisions (article 113(b)).

Which entities are to be designated market surveillance authorities?

EU Member States have some flexibility in designating market surveillance authorities; they can either establish a new body dedicated to enforcing the AI Act or integrate the requirements of the AI Act into the framework of an existing body already responsible for market surveillance under the EU harmonisation laws listed in Section A of Annex I or the existing bodies regulating financial or credit institutions regulated by EU law (article 74(3/6/7)). However, for high-risk systems in the area of biometrics, law enforcement, migration, asylum and border control management and the administration of justice, EU Member States must designate either the national Data Protection Authority established by the GDPR or the supervisory authority designated under Directive (EU) 2016/680 (article 74(8)).

Where AI systems relate to products already covered by the EU harmonisation legislation listed in Section A of Annex I and where such legal acts already provide for procedures ensuring an equivalent level of protection and having the same objective as the AI Act, the sectoral procedures shall apply instead of the national level enforcement procedures set out in articles 79 to 83 (see below under the heading 'Procedures for enforcement').

In this instance, dual reporting of serious incidents is not required and providers report under those other laws (article 73(9) and 73(10)). These exceptions specifically apply to:

- Annex III-type high-risk AI systems, where the provider is subject to EU law that establishes reporting obligations equivalent to those set out in the AI Act. Such equivalence may – for example – exist for critical infrastructure, which is covered by cybersecurity regulations that contain standalone incident reporting obligations that might be considered equivalent to those under the AI Act. However, it may not always be clear whether reporting obligations under other EU laws are considered equivalent to the reporting obligations under the AI Act; and

- high-risk AI systems that are safety components of devices, or are themselves devices, covered by Regulations (EU) 2017/745 on medical devices and (EU) 2017/746 on in vitro diagnostic medical devices. These both contain reporting obligations, according to which serious incidents must be reported to the competent authorities if they entail (a) the death of a patient, user or other person, (b) the temporary or permanent serious deterioration of a patient's, user's or other person's state of health, or (c) a serious public health threat.

However, in both instances, if the infringement relates to a violation of fundamental rights, it must still be notified under the AI Act, and the relevant market surveillance authority must inform the national fundamental rights authority/ authorities.

For AI systems used by EU institutions, agencies, offices, and bodies (with the exception of the CJEU acting in its judicial capacity), the European Data Protection Supervisor will be the market surveillance authority (article 74(9)).

Powers of the market surveillance authorities

The market surveillance authorities have all the broad enforcement powers set out in Regulation (EU) 2019/1020 in addition to further powers granted by the AI Act. For example, they have the power to:

- make operators disclose relevant documents, data and information on compliance. The AI Act adds that providers of high-risk AI systems may be compelled to disclose:

- training, validation and testing data sets used for the development of high-risk AI systems, including, where appropriate and subject to security safeguards, through application programming interfaces (API) or other relevant technical means and tools enabling remote access (article 74(12)); and

- where the testing or auditing procedures and verifications based on the data and documentation provided by the provider have been exhausted or proved insufficient, the source code if it is necessary to assess the conformity of a high-risk AI system with the requirements set out in chapter III, Section 2 (article 74(13));

- make unannounced on-site inspections and make test purchases (article 74(5));

- conduct investigations (engaging with the Commission where high-risk AI systems are found to present a serious risk across two or more EU Member States) (article 74(11));

- require operators to take appropriate actions to bring instances of non-compliance to an end, both formal non-compliance (article 83) and to eliminate a risk (articles 79-82);

- take appropriate measures where an operator fails to take corrective action or where the non-compliance persists, including withdrawal or recall (articles 73(8), 79-83); and

- impose penalties (articles 99-101).

The market surveillance authorities shall also ensure that testing in real world conditions is in accordance with the AI Act (see Chapter 7). They have the power to require the provider or deployer to modify the testing or suspend or terminate it (article 76(3)).

Handling of confidential information

Any information or documentation obtained by market surveillance authorities shall be treated in accordance with the confidentiality obligations set out in article 78. The provisions in article 78 also apply to the Commission, the authorities protecting fundamental rights and natural and legal persons involved in the application of the AI Act. Such persons shall carry out their tasks in a manner which not only protects confidential information and trade secrets, but also protects intellectual property rights and the rights in source code, public and national security interests and classified information.

These provisions are applying since 2 August 2025.

Procedures for enforcement

As already noted, the following procedures do not apply where there exists already harmonising legislation providing an equivalent level of protection and having the same objective as the AI Act.

AI systems presenting a risk (articles 79 and 81)

Where a market surveillance authority has sufficient reason to consider an AI system presents a risk (see definition above), it must carry out an evaluation as to whether the AI system is compliant with the AI Act.

If the it does not comply, the market surveillance authority shall without undue delay notify the relevant operator and require them to take all appropriate corrective actions to bring the AI system into compliance or to withdraw the AI system from the relevant market, or to recall it. The market surveillance authority shall state how long the operator has to comply, but it will be no longer than 15 working days.

If the operator does not take adequate corrective action by the end of the specified period, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict the AI system being made available on its national market or put into service, to withdraw the product or the standalone AI system from that relevant market or to recall it. The market surveillance authority must inform the operator of the grounds on which its decision is based.

Where the non-compliance is not restricted to its national territory, the market surveillance authority shall inform the Commission and the other EU Member States without undue delay of the results of the evaluation and of the actions which it has required the operator to take and the provisional measures which it has taken if the operator has not complied.

The provisional measures shall be deemed justified if no objection has been raised by either a market surveillance authority of an EU Member State or by the Commission within three months (reduced to 30 days in the event of non-compliance with the prohibitions referred to in article 5). However, if objections are raised, the Commission shall consult with the market surveillance authority and the operator or operators and, within six months (or 60 days for an article 5 issue), decide whether the provisional measure is justified. If it is, all EU Member States shall ensure that they take appropriate restrictive measures in respect of the AI system concerned, such as requiring withdrawal from their market. If it is not, the provisional measure will be withdrawn.

These provisions are without prejudice to the procedural rights of the operator set out in article 18 of Regulation (EU) 2019/1020, including the right to be heard.

AI systems classified by the provider as non-high-risk (article 80)

If the market surveillance authorities have sufficient reason to consider an AI system classified by the provider as non-high-risk under article 6(3) is indeed high-risk, it must carry out an evaluation.

The procedure to be followed is very much as described above, but article 80 specifically refers to the ability to fine the relevant provider.

In exercising their power to monitor the application of article 80, market surveillance authorities may take into account the information stored in the EU database of high-risk AI systems (see below under the heading 'Governance at EU Level: Role of the Commission').

Compliant AI systems which present a risk (article 82)

If a market surveillance authority finds that a high-risk AI system complies with the AI Act, but it nevertheless presents a risk to the health or safety of persons, to fundamental rights, or to other aspects of public interest protection, it shall require the relevant operator to take all appropriate measures to ensure that it no longer does so.

Formal non-compliance (article 83)

Where a market surveillance authority finds that, for example, a CE marking has not been affixed where it should, no authorised representative has been appointed or technical documentation is not available, it shall require the relevant provider to correct the matter within a prescribed period.

If the non-compliance persists, then the market surveillance authority shall take appropriate and proportionate measures to restrict or prohibit the high-risk AI system being made available on the market or to ensure that it is recalled or withdrawn from the market without delay.

Authorities protecting fundamental rights

In addition to identifying market surveillance authorities, by 2 August 2025, each EU Member State must identify the public authorities or bodies supervising and enforcing the obligations under EU law protecting fundamental rights, including the right to non-discrimination, in relation to the use of high-risk AI systems referred to in Annex III and shall notify them to the Commission.

Where market surveillance authorities identify risks to fundamental rights they must notify the relevant national public authority supervising their protection.

These bodies have the power to request and access any documentation created or maintained under the AI Act when access to that documentation is necessary for effectively fulfilling their mandates. The relevant public authority or body shall inform the market surveillance authority of the EU Member State concerned of any such request and, where the documentation proves insufficient may request the market surveillance authority to organise testing of the high-risk AI system through technical means (article 77).

General-purpose AI models

The Commission is the sole authority responsible for supervising and enforcing obligations on providers of general-purpose AI models. The rationale behind this is to benefit from centralised expertise and synergies at EU level (article 88). In practice, however, the AI Office (see below under the heading 'Governance') will carry out all necessary actions to monitor the effective implementation of the AI Act with regard to general-purpose AI models, provided that the organisational powers of the Commission and the division of competences between EU Member States and the EU are not affected.

The AI Office can investigate possible breaches of the rules by providers of general-purpose AI models on its own initiative, following the results of its monitoring activities, or at a request from market surveillance authorities.

It has the powers of a market surveillance authority for AI systems which are based on a general-purpose AI model, where the model and system are developed by the same provider.

Market surveillance authorities must cooperate with the AI Office to carry out compliance evaluations if a market surveillance authority considers that a general-purpose AI system (that can be used by deployers for at least one high-risk purpose) is non-compliant with the AI Act.

Market surveillance authorities can request the AI Office to provide information related to general-purpose AI models, where the market surveillance authority is unable to access that information (and as a result is unable to conclude its investigation into a high-risk system) (article 75).

Penalties

Any person, which fails to comply with the AI Act – whether a natural or legal person, a public authority or an EU or national institution – can be sanctioned for non-compliance. The provisions on penalties under the AI Act exceed even those provided for in the GDPR (which are up to EUR 20,000,000 or 4% of annual worldwide turnover). The maximum fine was revised throughout the legislative process but was ultimately set at EUR 35,000,000 or 7% of annual worldwide turnover.

Fines can be imposed by national authorities, the European Data Protection Supervisor, or the Commission. The European Data Protection Supervisor can impose fines on EU institutions, agencies and bodies. The Commission can impose fines on providers of general-purpose AI models. National authorities can impose fines on other operators.

The AI Act has a tiered approach to penalties, as shown below.

Grounds of infringement	EU bodies	All other persons
	Penalties imposed by EDPS	Penalties imposed by national authorities (unless GPAI models, in which case imposed by the Commission).
		For sanctioned persons which are undertakings, the penalties are capped at the higher of the %-based amount or the figure below. If the undertaking is an SME, they are capped at the lower amount. For other sanctioned persons, the specified figure is the cap.
Supplying incorrect, incomplete or misleading information to notified bodies or national competent authorities.	≤ €750,000 (article 100(3))	≤ 1% total worldwide annual turnover in preceding year; or ≤ €7,500,000 (article 99(5))
Obligations relating to high-risk AI systems.		≤ 3% of total worldwide annual turnover in preceding year; or ≤ €15,000,000 (article 99(4) for high-risk AI systems; article 101(1) for general-purpose AI models)
Obligations relating to providers of general -purpose AI models.		
Obligations relating to prohibited practices.	≤ €1,500,000 (article 100(2))	≤ 7% of total worldwide annual turnover in preceding year; or ≤ €35,000,000 (article 99(3))

No penalties are specified in the AI Act for failure to comply with the AI literacy obligations according to article 4. The enforcement has been left to national market surveillance authorities, which may provide for penalties under national law. A failure to ensure appropriate AI literacy may also be considered an aggravating factor when authorities assess compliance with other obligations under the AI Act.

Penalties and fines imposed by national authorities

It is the responsibility of EU Member States to provide for effective, proportionate, and dissuasive sanctions. These measures may include both monetary and non-monetary measures or warnings. They must be notified to the Commission by the date of entry into application (article 99(1) and (2)).

Penalties are to be imposed on a case-by-case basis. The competent national authority should consider all relevant circumstances of the specific situation, with due regard to the nature, gravity, and duration of the infringement and its consequences, as well as the size of the provider (article 99(7)).

Enforcement at EU Member State level must be subject to appropriate procedural safeguards, including effective judicial remedies.

Fines on EU institutions, bodies, offices and agencies

The European Data Protection Supervisor has the power to impose fines on EU institutions, agencies and bodies. Before adopting a decision on a fine, the EDPS should communicate its preliminary findings to the EU institution and

give it an opportunity to be heard. The fine is not to affect the effective operation of the institution and the funds collected by the imposition of fines are to be contributed to the general budget of the EU.

Fines on providers of general-purpose AI models

The Commission may impose fines on providers of general-purpose AI models for infringements (article 101). Unlike the other provisions on penalties and fines in chapter XII, which apply from 2 August 2025, article 101 does not apply until 2 August 2026.

The Commission will publish an implementing act with details on arrangements and procedural safeguards for proceedings.

When imposing a fixed amount or periodic penalty payment, the Commission should take due account of the nature, gravity and duration of the infringement, and the principles of proportionality and appropriateness. Before adopting a decision on a fine, the Commission should communicate its preliminary findings to the provider of the general-purpose AI model and give it an opportunity to be heard. The imposition of a fine must be subject to appropriate procedural safeguards, including judicial review before the CJEU. The CJEU may cancel, reduce or increase the amount of a fine imposed.

Remedies for third parties

Complaint to a market surveillance authority (article 85)

EU and EU Member State law already provide some effective remedies for natural and legal persons whose rights and freedoms are adversely affected by the use of AI systems. Notwithstanding, the AI Act introduces a new complaints mechanism. It mandates that any natural or legal person may submit a complaint to the competent market surveillance authority if it has grounds for believing there has been an infringement of the AI Act.

Under the GDPR, a data subject has the right to lodge a complaint with a supervisory authority about an alleged infringement if the data subject believes that the processing of personal data relating to him or her violates rights under the GDPR.

In contrast, a complaint lodged under the AI Act may concern not only an infringement of the rights of the complainant, but also compliance with the AI Act as a whole. In addition, under the GDPR a remedy can be filed only by the data subjects; under the AI Act, a complaint can also be filed by a legal person.

Right to explanation of individual decision-making (article 86)

Under the AI Act, any affected person is entitled to receive "clear and meaningful" explanations from the deployer concerning decisions made by high-risk AI systems (except for critical infrastructure systems). These explanations must clarify the decision-making procedure used and the main elements of the decision made by the AI system (article 86).

The right can be invoked if:

- a deployer's decision is mainly based on the output of high-risk AI systems; and
- that decision has legal effects or similarly significant effects on an affected person that adversely affect his or her health, safety or fundamental rights.

The right to an explanation under the AI Act aligns with a controller's obligation under the GDPR concerning automated decision-making processes (article 22 GDPR). Under the GDPR, the controller must provide the data subject with meaningful information on the logic and significance of the consequences of such processing.

Article 86 complements the data subject's right to an explanation under the GDPR; it is more specific to AI as it requires the deployer to explain the role of the AI system in the decision. In addition, the AI Act grants this right to all affected persons who can also be legal persons. National data protection authorities under the GDPR are still the competent authorities to enforce the controller's obligation to provide information when it comes to automated decision-making involving personal data processing, regardless of what authority is competent to enforce article 86.

Protection for whistleblowers (article 87)

Directive (EU) 2019/1937 on the protection of persons who report breaches of EU law applies to the reporting of infringements of the AI Act.

Downstream providers' complaint (article 89)

The AI Act enables complaints by downstream providers (deployers of general-purpose AI systems) about possible violations of the rules set out in the Act.

Complaints can be made to the AI Office and must be well-substantiated. They should include at least:

- details of the provider of the general-purpose AI model that is the subject of the complaint, and its point of contact;
- a description of the relevant facts, together with the provisions that have been breached;
- the reasons why the complainant believes there has been an infringement; and
- any other information that the requesting downstream provider deems relevant, including, where appropriate, information gathered at its own initiative.

The possibility for downstream providers to make such complaints enables the AI Office to effectively oversee the enforcement of the AI Act.

Governance

The governance structure has been established to coordinate and support the application of the AI Act. Its aim is to build capabilities at both EU and national levels, integrate stakeholders, and ensure trustworthy and constructive cooperation.

Governance at EU Level: role of the Commission

The Commission is tasked by the AI Act with many responsibilities including developing and implementing delegated acts, developing and publishing guidelines, setting standards and best practice and making binding decisions to implement the AI Act effectively. In practice, these tasks will be carried out by the AI Office, which is part of the administrative structure of the Directorate-General for Communication Networks, Content and Technology, in its role of supporting the Commission.

One of the tasks that the Commission, in collaboration with the EU Member States, must perform is set out in Chapter VIII. The Commission must set up and maintain an EU database for high-risk AI systems referred to in article 6(2) and AI systems that are not considered as high-risk pursuant to article 6(3). The database will contain:

- the data listed in Sections A and B of Annex VIII entered into the EU database by the provider or the authorised representative; and
- the data listed in Section C of Annex VIII entered into the EU database by the deployer who is, or who acts on behalf of, a public authority, agency or body.

The data will be available to the public (with the exception of data relating to AI systems in the areas of law enforcement, migration, asylum and boarder control management).

The supranational bodies set up by the AI Act

Role of the AI Office	Actions
The AI Office was established by the Commission by its decision of 24 January 2024 (C/2024/1459). The AI Office's function is to oversee the advancements in AI models, including as regards general-purpose AI models, the interaction with the scientific community, and to play a key role in investigations and testing, enforcement and to have a global vocation (recital 5 of the decision). The AI Office may involve independent experts to carry out evaluations on its behalf. The AI Office must establish systems and procedures to manage and prevent potential conflicts of interest and must develop EU expertise and capabilities in the field of AI. The AI Office has a role in the surveillance and control of general-purpose AI systems (article 75).	**Monitoring and enforcement:** Monitor compliance and implementation of obligations for providers of general-purpose AI models. **Investigation:** Investigate infringements by requesting documentation and information, conducting evaluations and requesting measures from providers of general-purpose AI models. **Risk management:** Request appropriate measures, including risk mitigation, in cases of identified systemic risks, as well as restricting market availability, withdrawing or recalling the model. **Coordination and support:** Support national authorities in creating AI regulatory sandboxes and facilitate cooperation and information-sharing and encourage and facilitate the creation of codes of conduct. Coordinate joint investigations by market surveillance authorities and the Commission. **Advice:** Issue recommendations and written opinions to the Commission and the Board regarding codes of conduct, codes of practice and guidelines.

Role of the Board	Actions
The Board comprises representatives from each EU Member State and is tasked with advising and assisting the Commission and the EU Member States on the consistent and effective application of the AI Act. Additionally, the Board issues guidelines and recommendations (articles 65 and 66). Representatives are appointed for a term of three years, renewable once. They may be individuals from public entities with expertise in AI and the authority to facilitate national-level coordination. The Board is chaired by one of its representatives.	**Coordination and cooperation:** Among national competent authorities and EU institutions, bodies, offices and agencies, as well as relevant EU expert groups and networks. **Expertise sharing:** Collect and share technical and regulatory expertise, best practices and guidance documents. **Advice and recommendations:** Provide advice on the implementation of the AI Act, in particular as regards the enforcement of rules on general-purpose AI models, issue recommendations and written opinions (at the request of the Commission or on its own initiative).

Role of the Board	Actions
The Board must establish two dedicated standing subgroups: • The standing subgroup for notifying authorities provides a platform for cooperation and exchange on issues related to notified bodies. • The standing subgroup for market surveillance acts as the administrative cooperation group (ADCO) for the AI Act. The Board may establish other standing or temporary subgroups as appropriate for the purpose of examining specific issues. The European Data Protection Supervisor and the AI Office attend the Board's meetings as observers. Other national and EU authorities, bodies, or experts or representatives of the advisory forum may be invited on a case-by-case basis.	**Harmonisation:** Standardise administrative practices and facilitate the development of common criteria and a shared understanding. **Public awareness on AI:** Work towards AI literacy, public awareness and understanding of the benefits, risks, safeguards and rights and obligations in relation to the use of AI systems. **International Cooperation:** Advise the Commission in relation to international matters on AI and cooperate with competent authorities of third countries and with international organisations.

Role of the Advisory Forum	Actions
The Advisory Forum has been created to ensure the involvement of stakeholders in the implementation and application of the AI Act (article 67). Members are appointed by the Commission and represent a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society, and academia with recognised expertise in the field of AI. Members are appointed for a term of two years, which may be extended up to four years. They elect two co-chairs from among the members for a term of two years, renewable once. The Fundamental Rights Agency (FRA), the European Union Agency for Cybersecurity (ENISA), the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI) shall be permanent members of the Advisory Forum. The Advisory Forum may establish standing or temporary sub-groups as appropriate for examining specific questions. The Advisory Forum meets at least twice a year and may invite experts and other stakeholders to its meetings.	**Advice and technical expertise:** Provide advice to the Board and the Commission. Prepare opinions, recommendations, and written contributions upon request. **Consultancy group:** The Commission has to consult the Forum when preparing a standardisation request or drafting common specifications as referred to in article 41. **Annual report:** Prepare and publish an annual report on its activities.

Role of the scientific panel of independent expert	Actions
The scientific panel is created to integrate the scientific community in supporting the Commission's enforcement activities (article 68). Experts are selected by the Commission based on their current scientific or technical expertise in AI. The number of experts is determined by the Commission, in consultation with the Board, based on the required expertise needs, ensuring fair gender and geographical representation. To provide the scientific panel with the necessary information for performing its tasks, a mechanism should be established allowing the panel to request the Commission to obtain documentation or information from a provider. An implementing act will define how the scientific panel and its members can issue alerts and request assistance from the AI Office.	Support the AI Office in the implementation and enforcement as regards general-purpose AI models and system: • Alert the AI Office of possible systemic risks. • Develop tools and methodologies for evaluating capabilities. • Advise on the classification including systemic risk. • Contribute to the development of tools and templates. • Support market surveillance authorities: At their request including with regard to cross-border market surveillance activities. • Assist in the EU safeguard procedure pursuant article 81. Support EU Member States with their enforcement activities upon demand: • EU Member States may be required to pay fees for the advice and support provided by the scientific panel. • The implementing act referred to in article 68(1) will define the fees and recoverable costs.

Governance at national level: national competent authorities

EU Member States play a crucial role in the application and enforcement of the AI Act. To ensure effective application, harmonisation, and coordination within the EU and among EU Member States, each EU Member State must designate at least one notifying authority and one market surveillance authority. Together, they constitute the national competent authorities. For AI systems used by EU institutions, agencies, offices, and bodies, the European Data Protection Supervisor will be the supervisory authority.

Role of the notifying authority(ies)	Actions
This authority is responsible for establishing and applying the framework for conformity assessment bodies (article 28). The authority must have an adequate number of competent personnel with the necessary expertise in fields such as information technology, AI, and law, including the supervision of fundamental rights. Notifying authorities must avoid any conflict of interest with conformity assessment bodies, ensuring the objectivity and impartiality of their activities. In particular, the decision to notify a conformity assessment body must not be made by the person who assessed the conformity assessment body.	Setting up and carrying out procedures: Establish and execute necessary procedures for the assessment, designation, notification, and monitoring of conformity assessment bodies. Develop these procedures in cooperation with the notifying authorities of other EU Member States. Advice and guidance: Provide guidance and advice on the implementation of the AI Act, considering the input from the Board and the Commission, and consulting national competent authorities under other EU laws, if applicable. Activity and service restrictions: • Must not offer or provide any activities performed by conformity assessment bodies. • Must not offer consultancy services on a commercial or competitive basis.

Role of the market surveillance authority(ies)	Actions
Responsible for carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020 (market surveillance and compliance of products) on market surveillance and compliance of products. One of the market surveillance authorities will be designated by each EU Member State as the single point of contact for the public and other counterparts at both EU Member State and EU levels. The European Data Protection Supervisor will act as the market surveillance authority for EU institutions, agencies, and bodies under the AI Act. Market surveillance authorities for high-risk AI systems in biometrics, used for law enforcement, migration, asylum, border control, justice, and democratic processes, should have strong investigative and corrective powers. This includes access to all personal data and necessary information for their task. EU Member States must facilitate coordination between market surveillance authorities and other relevant national authorities.	Many of task and responsibilities of the market surveillance authorities are described above, but in addition they have the following tasks and responsibilities assigned to them: • Authorisation for high-risk AI systems: EU Member States can temporarily authorise specific high-risk AI systems to be placed on the market or put into service in their territory for exceptional reasons of public security, health, environmental protection, or key infrastructure, pending conformity assessments (article 46). • Annual reporting: to the Commission and national competition authorities on surveillance activities and prohibited practices including: (i) any information identified that is of potential interest for the application of competition law; (ii) use of any prohibited practices; and (iii) measures taken in relation to those practices. • Advice and guidance: Provide guidance and advice on the implementation of the AI Act, considering the input from the Board and the Commission, and consulting national competent authorities under other EU laws, if applicable.

Where can I find this?

Governance: Chapter VII	recitals 148-154, 163,179
EU Database: Chapter VIII	recital 131
Enforcement: Chapters IX and XII	recitals 162-164 and 168-172

AI Act: What's Next

At a glance

- The AI Act entered into force on 1 August 2024.
- Most provisions are set to apply from 2 August 2026, and others are being phased in over a period of six to 36 months from the date of entry into force.
- The Commission will develop delegated and implementing acts, guidelines, Codes of Practice. These initiatives are aimed at providing practical guidance, ethical principles and technical specifications related to the AI Act, with the goal of ensuring the effective implementation of the legislation.
- CEN and CENELEC are working on technical standards to support implementation of obligations under the AI Act.
- The Commission withdrew its proposal for an AI Liability Directive in October 2025.
- The Commission's Digital Omnibus proposal, issued in November 2025 would adjust the timing for key AI Act obligations, notably postponing certain high-risk requirements that, at time of writing, are still due to apply from 2 August 2026 and linking their application to the availability of supporting standards, common specifications or guidelines. Under the proposal, high-risk obligations for AI systems listed in Annex III could apply no earlier than six months after a Commission "tools ready" decision (with a long-stop of 2 December 2027), while obligations for systems requiring harmonised product legislation would apply 12 months after that decision (with a long-stop of 2 August 2028).
- Bird & Bird's AI experts are equipped to monitor the forthcoming initiatives expected under AI Act and help you navigate the different processes and requirements.

To do list

- [ ] All actors dealing with AI systems should actively monitor the development of the legislative and non-legislative initiatives outlined in this chapter.

AI Act: What's Next

This chapter provides an overview of the forthcoming initiatives expected under the AI Act. The EU institutions regard the AI Act as a new form of "living regulation" that will be supplemented on an ongoing basis via secondary legislation and other initiatives, in an effort to keep pace with technological advances. The AI Act envisions and the Commission has been and is continuing to adopt various a range of delegated and implementing acts, guidance documents, codes of conduct, Codes of Practice and standardisation requests. These initiatives are designed to provide practical guidance, ethical principles and technical specifications regarding the AI Act, with the aim of ensuring effective implementation and the ability of actors to comply with its obligations.

All actors dealing with AI systems would therefore be advised to actively monitor the work of the Commission in developing the legislative and nonlegislative initiatives mentioned in this chapter.

Bird & Bird's AI experts are equipped to monitor the forthcoming initiatives expected under AI Act and help you navigate the different processes and requirements.

Delegated acts

Several provisions have been and will continue to be the subject of delegated acts, to be adopted by the Commission to specify obligations and operational implementation. Article 97 grants the power to adopt delegated acts to the Commission for a five-year period that started on 1 August 2024. The Commission must report on this delegation nine months before the end of the period. This period is automatically extended for another five years unless the European Parliament or the Council opposes it three months before the end of each period.

Pursuant to article 97(4), before adopting a delegated act, the Commission has been carrying out and will likely continue to carry out public consultations during its preparatory work and will also consult with the relevant Expert Groups (composed of EU Member States experts).

Once adopted, the Commission must notify the European Parliament and the Council simultaneously. A delegated act only enters into force if neither the European Parliament nor the Council objects within three months of notification, extendable by another three months if needed. The European Parliament or the Council can revoke this power at any time, but this will not affect the validity of existing delegated acts. In accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law Making[4], the Commission will have to ensure that the European Parliament and the Council receive all documents at the same time as EU Member States' experts, and the Parliament and Council's experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

The AI Act foresees the adoption of the following delegated acts where the Commission considers this to be necessary:

- **Article 6(6/7)**: amend article 6(3) by adding new conditions to those laid down in paragraph 3, by modifying or by deleting them if there is concrete and reliable evidence of the existence of AI systems that should not fall under Annex III or that should not fall under the conditions of article 6(3);
- **Article 7(1/3)**: amend Annex III, by adding, modifying or removing use-cases of high-risk AI systems;
- **Article 11(3)**: amend Annex IV, where necessary, to ensure that, in light of technical progress, the technical documentation provides all the information necessary to assess the compliance of the system;
- **Article 43(5)**: amend Annexes VI and VII by updating them in light of technical progress;
- **Article 45(6)**: amend article 43(1/2) in order to subject high-risk AI systems referred to in points 2 to 8 of Annex III to third-party conformity assessments;
- **Article 47(5)**: amend Annex V by updating the content of the EU declaration of conformity set out in that Annex, in order to introduce elements that become necessary in light of technical progress;

4. Inter-institutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making, OJ L 123, 12.5.2016.

- **Article 51(3)**: amend the thresholds for systemic general-purpose AI models listed in article 51(1/2) as well as to supplement benchmarks and indicators in light of evolving technological developments, such as algorithmic improvements or increased hardware efficiency, when necessary, for these thresholds to reflect the state of the art;
- **Article 52(4)**: amend Annex XIII by specifying and updating the criteria for systemic general-purpose AI models;
- **Article 53(5)**: detail measurement and calculation methodologies with a view to allowing for comparable and verifiable documentation to facilitate compliance with Annex XI; and
- **Article 53(6)**: amend Annexes XI and XII in light of evolving technological development.

Implementing acts

Article 98(2) confers on the Commission the power to adopt implementing acts in accordance with Regulation 182/2011[5]. Implementing acts aim to create uniform conditions for the implementation of a specific legislative act, if and when this is necessary. With respect to the drafting of the implementing acts, the Commission will be assisted by a *"Comitology"* Committee comprising EU Member State experts.

As is the case for delegated acts, the timeline for adoption of the expected implementing acts is not specified in the text, except for the foreseen implementing act referred to in article 72(3), which was due by 2 February 2026. Therefore, it should be presumed that the relevant implementing acts will be adopted ahead of the application deadlines for the related provisions in the AI Act (see above and article 113).

The AI Act foresees the adoption of the following implementing acts, where the Commission deems it necessary to:

- **Article 37(2)**: suspend, restrict or withdraw the designation of notified bodies when the EU Member State fails to take the necessary corrective measures;
- **Article 41(1/4/6)**: establish, in consultation with the *"Advisory Forum"* referred to in article 67, common specifications for the requirements for high-risk AI systems or for the obligations for general-purpose AI models set out in Chapter V, Sections 2 and 3. When a reference to a harmonised standard is published in the Official Journal of the EU, which covers the same requirements set out in Section 2 of this Chapter III, the Commission shall repeal the implementing act referred to in article 41(1). Where an EU Member State considers that a common specification does not entirely meet the requirements set out in Section 2 of this Chapter III, the Commission shall assess that information and, if appropriate, amend the implementing act referred to in article 41(1);
- **Article 50(7)**: approve codes of practice drawn up to facilitate the effective implementation of the obligations regarding the detection and labelling of artificially generated or manipulated content, in accordance with the procedure laid down in article 56(6). A first draft of the Code of Practice was published in December 2025. If the final Code of Practice is not adequate, the Commission may adopt an implementing act to lay down a set of common rules for the implementation of the transparency obligations for providers and deployers of certain AI systems of article 50;
- **Article 56(6)**: approve a Code of Practice for general-purpose AI models and give it a general validity within the EU. The Code of Practice for general-purpose AI models was approved by the Commission on 1 August 2025;
- **Article 58(1)**: specify the detailed arrangements for the establishment, development, implementation, operation and supervision of the AI regulatory sandboxes;
- **Article 60(1)**: specify the detailed elements of the real-world testing plan for providers of high-risk AI systems;

5. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by EU Member States of the Commission's exercise of implementing powers, OJ L 55, 28.2.2011.

- **Article 68(1)**: make provisions on the establishment of a scientific panel of independent experts intended to support the enforcement activities of the AI Act;
- **Article 72(3)**: publish, by 2 February 2026, an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan for providers of high-risk AI systems and the list of elements to be included in the plan;
- **Article 92(6)**: set out the detailed arrangements and the conditions for the AI Office of general-purpose AI models evaluations, including the detailed arrangements for involving independent experts, and the procedure for the selection thereof; and
- **Article 101(6)**: lay down detailed arrangements and procedural safeguards for proceedings in view of the possible fines on providers of general-purpose AI models.

Commission Guidelines

Commission Guidelines are non-binding explanatory documents adopted by the Commission (or published by the Commission services) to provide practical and informal guidance on the interpretation and application of specific provisions of the AI Act. While they do not have the force of law, they play a significant role in shaping enforcement practice and compliance approaches across the EU.

As at the time of writing, the Commission has published the following Guidelines:

- Guidelines on prohibited artificial intelligence (AI) practices (article 5), published on 4 February 2025;
- Guidelines on AI system definition (article 3(1)), published on 6 February 2025; and
- Guidelines on the scope of obligations for providers of general-purpose AI models (articles 51-55), published on 18 July 2025.

The AI Act also foresees the adoption of the following Commission Guidelines:

- Guidelines on the classification of high-risk AI systems (article 6);
- Guidelines on the application of the requirements and obligations for high-risk AI systems (including responsibilities along the AI value chain) (articles 8-15 and 25);
- Guidelines on the practical implementation of the provisions related to substantial modification (article 96(1));
- Guidelines on the practical implementation of transparency obligations laid down in article 50;
- Guidelines on reporting serious incidents to market surveillance authorities under article 73 (article 73(7));
- Guidelines on a simplified quality management system for high-risk AI systems for microenterprises (article 63); and
- Detailed information on the relationship of the AI Act with the EU harmonisation legislation listed in Annex I, as well as with other relevant EU law, including as regards consistency in their enforcement (article 96(1)).

Codes of Conduct and Practice

Codes of conduct are documents of a voluntary nature that establish ethical guidelines and principles for the development and use of AI in certain conditions. They are also intended to foster the development of AI policies within organisations for the voluntary application of specific AI Act obligations.

The AI Act calls for the adoption of the following codes of conduct:

- **Recital 20 and article 4:** voluntary codes of conduct to advance AI literacy among persons dealing with the development, operation and use of AI.
  - While there is no set deadline for the development of voluntary codes of practice

to advance AI literacy, the related provisions on AI literacy in Article 4 will apply from 2 August 2026.

- **Recital 165 and article 95:** codes of conduct intended to foster the voluntary application to AI systems of some or all the mandatory requirements applicable to high-risk AI systems. These are adapted in light of the intended purpose of the systems and the lower risk involved, and take into account the available technical solutions and industry best practices such as model and data cards:
  - to ensure that the voluntary codes of conduct are effective, they should be based on clear objectives and key performance indicators to measure the achievement of those objectives;
  - they should also be developed in an inclusive way, as appropriate, with the involvement of relevant stakeholders such as business and civil society organisations, academia, research organisations, trade unions and consumer protection organisations; and
  - while there is no set deadline for the development of voluntary codes of practice intended to foster the application to AI systems of some or all the mandatory requirements applicable to high-risk AI systems, the related provisions included in Article 95 will apply from 2 August 2026. By 2 August 2028 and every three years thereafter, the Commission is due to evaluate the impact and effectiveness of such voluntary codes of conduct.

Codes of Practice

Codes of practice represent a central tool for proper compliance with specific obligations under the AI Act. In particular, the AI Act envisions a Code of Practice which will detail the AI Act rules for providers of general-purpose AI models and general-purpose AI models with systemic risks. It further envisions another Code of Practice which will focus on the detection and labelling of artificially generated or manipulated content. Organisations should be able to rely on Codes of Practice to demonstrate compliance with the relevant obligations, which is known as a "*presumption of conformity*".

Specifically, the AI Act calls on the AI Office to facilitate the drawing up of the following codes of practice together with all interested stakeholders:

- **Article 50(7):** A Code of Practice for the AI-generated content and the obligations under articles 50(2) and (4) is currently under development as is expected to be finalised before these provisions come into force on 2 August 2026.
- **Article 56(1/3):** A Code of Practice for providers of general-purpose AI models was published on 10 July 2025 and approved by the Commission on 1 August 2025.

By 2 August 2028 and every three years thereafter, the Commission will have to evaluate the impact and effectiveness of voluntary codes of conduct.

Standards

Initial standardisation work

The process of drafting European standards in support of the AI Act started well before the adoption of the AI Act, with the Commission's proposal on harmonised rules on artificial intelligence adopted as the Commission Implementing Decision C(2023)3215 on 22 May 2023.

This Implementing Decision requested the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) to draft the following new European standards or European standardisation deliverables on AI by 30 April 2025:

- European standard(s) and/or European standardisation deliverable(s) on risk management systems for AI systems;
- European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems;
- European standard(s) and/or European standardisation deliverable(s) on record keeping through logging capabilities by AI systems;

- European standard(s) and/or European standardisation deliverable(s) on transparency and information provisions for users of AI systems;
- European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems;
- European standard(s) and/or European standardisation deliverable(s) on accuracy specifications for AI systems;
- European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems;
- European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems;
- European standard(s) and/or European standardisation deliverable(s) on quality management systems for providers of AI systems, including post-market monitoring processes; and
- European standard(s) and/or European standardisation deliverable(s) on conformity assessment for AI systems.

This standardisation request to CEN and CENELEC was made pursuant to action 63 of the Commission 2022 "Annual Union Work Programme for European standardisation" with the aim of ensuring that AI systems are safe and trustworthy.

For the drafting of these standards, CEN and CENELEC have set up a specific joint technical committee named *"CEN-CENELEC JTC 21 Artificial Intelligence"*. CEN and CENELEC are also collaborating on the drafting with the European Telecommunications Standards Institute (ETSI), an independent, not-for-profit, standardisation organisation in the field of information and communication. At the time of writing the deadline of 30 April 2025 has not been met. In October 2025, CEN and CENELEC adopted an exceptional package of measures to accelerate the delivery of key standards required under the standardisation request.

By 2 August 2028 and every four years thereafter, the Commission will have to submit a report to review the progress made regarding the development of standardisation deliverables on the energy-efficient development of general-purpose AI models. In this context, the Commission will also be required to assess the need for further measures or actions, including binding measures or actions. The report will have to be submitted to the European Parliament and to the Council and made public.

AI Guide Contributors

As a market-leading law firm for technology, ranked Tier 1 for AI (first ranking of its kind within the European legal directory community) and TMT by Legal 500 in 12 jurisdictions and Band 1 for global multi-jurisdictional TMT by Chambers, we distinguish ourselves through our deep understanding of the technical intricacies involved in AI technology development and deployment. This expertise enables us to effectively collaborate with developers and commercial teams, speaking their language and asking the right questions from the outset. Our international AI group comprises over **120 experts**, covering virtually every intersection where this transformative technology meets law and regulation. From handling ground-breaking IP litigation and guiding clients through complex regulatory changes to implementing effective governance frameworks and innovating commercial and contractual arrangements.

If you have any questions about the content, please get in touch with any of the contributors below or your usual Bird & Bird contact. You can also find out more about the latest AI developments in our AI Hub

Belgium

Benoit Van Asbroeck
Of Counsel

+3222826067
benoit.van.asbroeck@twobirds.com

Paolo Sasdelli
Regulatory and Public Affairs Advisor

+3222826076
paolo.sasdelli@twobirds.com

Finland

Tobias Bräutigam
Partner

+358962266758
tobias.brautigam@twobirds.com

France

Anne-Sophie Lampe
Partner

+33142686333
anne-sophie.lampe@twobirds.com

Cen Zhang
Senior Associate

+33142686000
cen.zhang@twobirds.com

Germany

Dr. Miriam Ballhausen
Partner

+4940460636000
miriam.ballhausen@twobirds.com

Dr. Nils Lölfing
Counsel

+4921120056000
nils.loelfing@twobirds.com

Oliver Belitz
Counsel

+4969742226000
oliver.belitz@twobirds.com

Dr. Simon Hembt
Counsel

+4969742226000
simon.hembt@twobirds.com

Italy

Gian Marco Rinaldi
Counsel

+390230356071
gianmarco.rinaldi@twobirds.com

Andrzej Stelmachowski
Associate

+48225837977
andrzej.stelmachowski
@twobirds.com

Pawel Lipski
Partner

+48225837991
pawel.lipski@twobirds.com

Poland

Aleksandra Cywinska
Senior Associate

+48225837875
aleksandra.cywinska@twobirds.com

Izabela Kowalczuk-Pakula
Partner

+48225837932
izabela.kowalczuk-pakula@
twobirds.com

Spain

Joaquín Muñoz
Partner

+34917906007
joaquin.munoz@twobirds.com

Aleksandra Mizerska
Lawyer

+48225837900
aleksandra.mizerska@twobirds.com

Marta Kwiatkowska-Cylke
Counsel

+48225837964
marta.kwiatkowska-cylke@
twobirds.com

The Netherlands

Feyo Sickinghe
Of Counsel

+31703538904
feyo.sickinghe@twobirds.com

United Kingdom

Alex Jameson
Senior Associate

+442078507139
alex.jameson@twobirds.com

Ian Edwards
Partner

+442079056377
ian.edwards@twobirds.com

Katharine Stephens
Partner

+442074156104
katharine.stephens@
twobirds.com

United Kingdom

Liz McAuliffe
Associate

+442074156787
liz.mcauliffe@twobirds.com

Nora Santalu
Associate

+442079826513
nora.santalu@twobirds.com

Ruth Boardman
Partner

+442074156018
ruth.boardman@twobirds.com

Toby Bond
Partner

+442074156718
toby.bond@twobirds.com

Will Bryson
Partner

+442074156746
will.bryson@twobirds.com

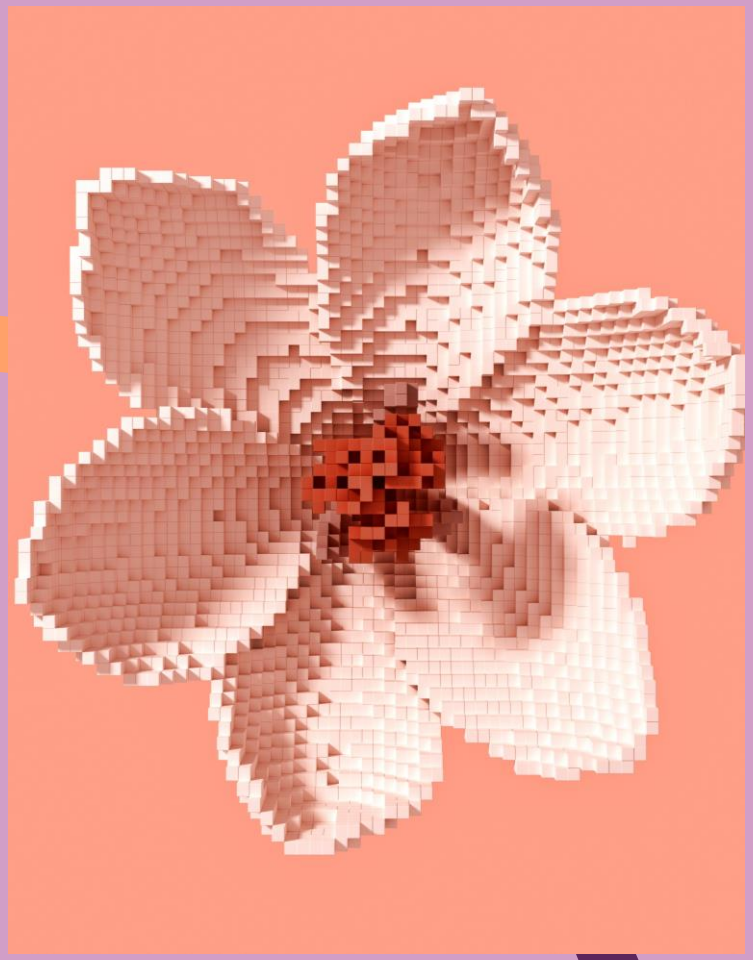
twobirds.com

Bird & Bird

Bird & Bird

AI Across the Atlantic

Navigating Divergent US and EU Legal Frameworks



AI Across the Atlantic

Navigating Divergent US and EU Legal Frameworks

Michelle Huang

Frontier Counsel, Anthropic

Jordan Gimbel

Associate General Counsel, Microsoft

Izabela Kowalczuk-Pakula

Partner, Bird & Bird

izabela.kowalczuk-pakula@twobirds.com

Vincent Rezzouk-Hammachi

Partner, Bird & Bird

vincent.rezzouk@twobirds.com

Chris de Mauny

Partner, Bird & Bird

chris.demauny@twobirds.com

Bird & Bird

1. 2025 in review
   - Key developments and lessons learned
2. 2026 outlook
   - Upcoming compliance deadlines and regulatory changes
3. The Digital Omnibus Package and its proposed amendments
4. Practical steps for implementing high-risk AI systems

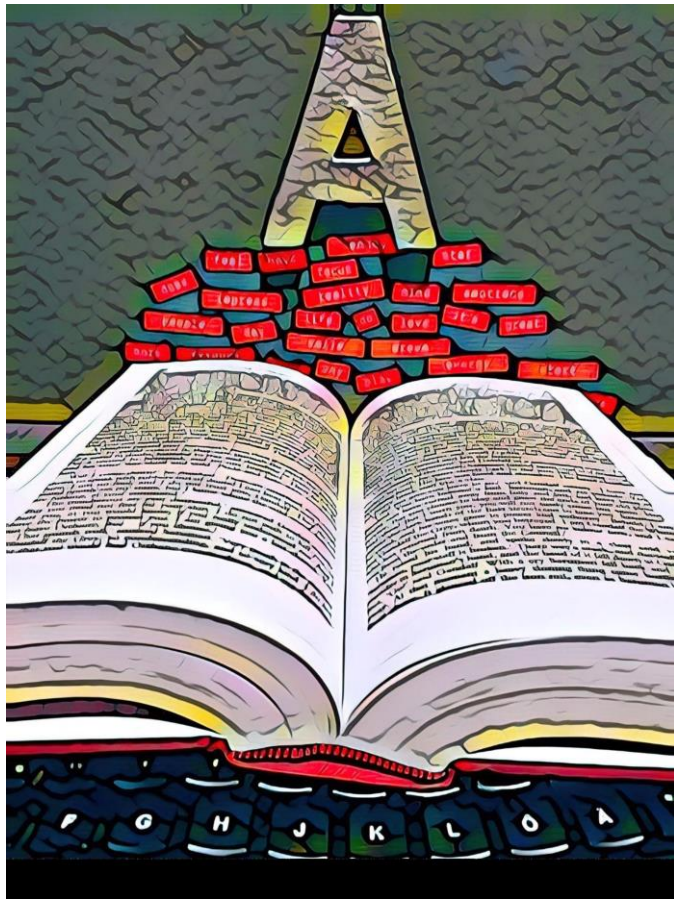
1 **2025 in review** – key developments and lessons learned

The first AI Act obligations came into force

2 February 2025

Prohibitions on AI practices (Article 5) came into force **but,** the provisions on governance and penalties only came into effect on 2 August 2025.

AI literacy obligation under Article 4 also came into force for providers and deployers of AI systems **but,** no specific sanctions for breach are set out in the AI Act, leaving it to member states to decide whether to introduce penalties in national implementing legislation.



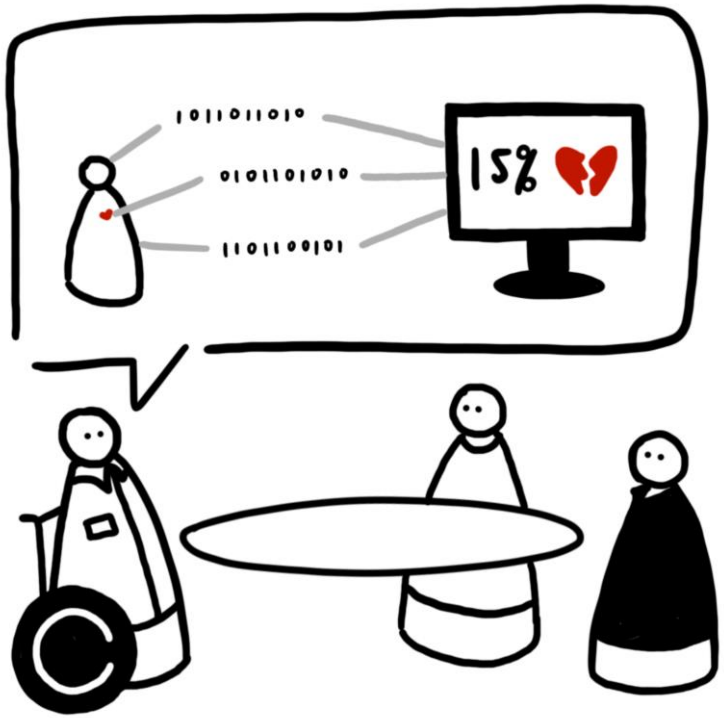
Teresa Berndtsson / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

The first Commission Guidelines clarified the AI Act scope and prohibitions

4 and 6 February 2025

The Commission published its first guidelines on:

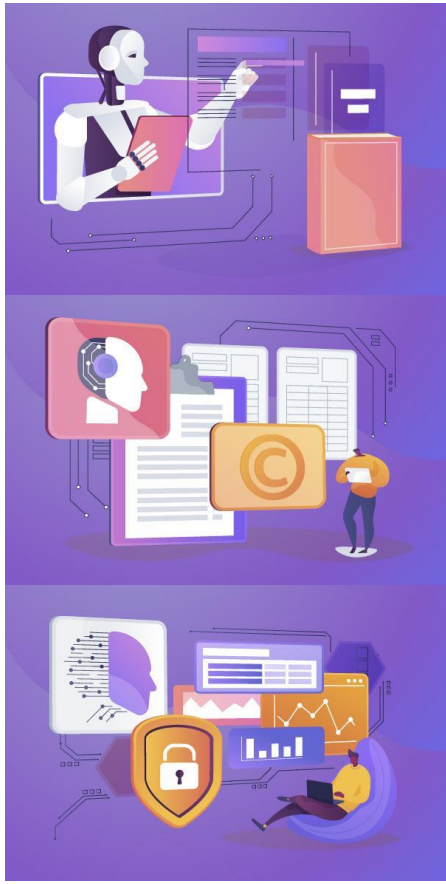
- **definition of an AI system**
- **prohibited practices**.



Yaning Wu / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

General-purpose AI models were the next regulatory focal point (1)

July – August 2025



GPAI model provider obligations (Articles 51-55) came into force on 2 August 2025… **But**, only for GPAI models placed on the EU market after that date (models on the EU market before have until 2 August 2027) (Article 111(3)) … **And** the Commission's powers to enforce the rules only come into effect on 2 August 2026 (Article 113).

Prior to the deadline, extensive work by four working groups culminated in the publication a **GPAI Code of Practice** (10 July 2025) … which the Commission and the AI Board confirmed are an adequate voluntary tool for providers of GPAI models to demonstrate compliance with the AI Act.

Three chapters: Transparency, Copyright, Safety and Security

After some industry concerns about the burden and timing of **the GPAI Code of Practice**, 28 GPAI model providers have so far signed all three chapters of Code of Practice (with one additional provider signing only the Safety and Security chapter).

General-purpose AI was the next regulatory focal point (2)

July - August 2025

After a consultation on a "provisional approach" in April 2025, the Commission published **Guidelines on the scope of obligations for providers of general-purpose AI models** (18 July 2025).

This was following by a **training data disclosure template** under Article 53(1)(d) (24 July 2025).

Beckett LeClair / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Harmonised standards fell behind, then tried to catch up

October 2025

The Commission's standardisation request in 2023 asked CEN and CENELEC to produce harmonised standards by 30 April 2025

In June 2025, these standardisation bodies were predicting that most standards would be ready in the summer of 2026…

In October 2025 CEN and CENELEC adopted an exceptional package of measures to accelerate the delivery of key standards required under the standardisation request

Leo Lau & Digit / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Lessons learned from AI Act developments in 2025

- The AI Act has gaps - guidelines are essential to fill them
- Codes of Practice are being used to create extensive "soft law" requirements
- The AI Office has a huge amount of work to do preparing guidelines and supporting development of Codes of Practice - it has kept the show on the road in 2025 (after an early wobble…)
- Engaging with the process is important: consultations on guidelines are generally resulting in improvements
- The AI Office wants to take a collaborative, staged and proportionate approach to enforcing GPAI requirements

Zoya Yasmine / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

2

2026 outlook – upcoming compliance deadlines and regulatory changes

Upcoming deadlines

High risk AI systems and AI systems with transparency risks

Obligations for **high-risk AI systems** (Annex III – high-risk use cases) apply from **2 August 2026**

- For AI systems placed on the market from **2 August 2026**, and AI systems placed on the market prior that have undergone **significant changes** (*substantial modification*)
- Not only for **providers** of high-risk AI systems, but also other operators (**deployers, importers, distributors**)
- See Articles 23 - 26

Obligations for **AI systems with transparency risks** (chatbots, generative AI systems) apply from **2 August 2026**

- **Providers:** transparent AI-chatbots; labelling AI-generated content
- **Deployers:** disclosing use of emotion recognition/biometric categorisation systems and use of 'deep fakes'

Obligations for **high-risk AI systems** that qualify as **safety components** apply from **2 August 2027**

Guidance – Recent developments

Transparency requirements of Article 50

- First draft of the **Code of Practice** for the **transparency obligations** of Article 50 published in December (adoption May – June)
  - **Section 1**: Commitments for the **labelling** of **AI-generated content** (for **providers**)
    1. Multi-layered marking of AI-generated content
    2. Detection of the marking of AI-generated content
    3. Measures to meet the requirements for marking and detection technique
    4. Testing, verification and monitoring

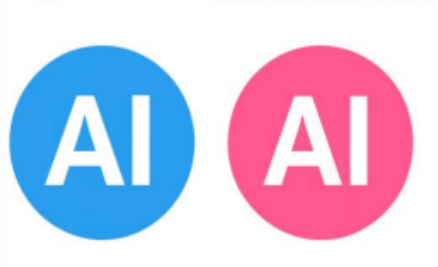
Guidance – Recent developments

Transparency requirements of Article 50

- First draft of the **Code of Practice** for the **transparency obligations** of Article 50 published in December (adoption May – June)
  - **Section 2**: Commitments for the **labelling** of **deepfakes** and **AI-generated text** (for **deployers**)
    1. Disclosure of origin of AI-generated content based on common taxonomy
    2. Compliance, training and monitoring
    3. Ensure accessible disclosure for all natural persons
    4. Specific measures for deepfake disclosure
    5. Specific measures for AI-generated text

The indication of the two-level taxonomy in an icon with the AI-acronym

To support consistent disclosure, a two-letter acronym referring to artificial intelligence should be used, which can also reflect the relevant translation in the languages of the Member States (e.g. AI, KI, IA).



Appendix 1 of the Draft CoP

Guidance – What can be expected?

Guidelines on …

- the practical application of the **high-risk classification**
- the practical application of the **transparency requirements** under Article 50 AI Act (in addition to the CoP)
- the reporting of **serious incidents** by providers of high-risk AI systems
  - *Draft + template for reporting published in September*
- the practical application of the **high-risk requirements**
- the practical application of the **obligations for providers and deployers** of high-risk AI systems
- a template for the **fundamental rights impact assessment**
- the practical application of rules for **responsibilities along the AI value chain**
- the practical application of the provisions related to **substantial modification**
- providing a voluntary template for the **post-market monitoring** of high-risk AI systems
- the elements of the **quality management system** which **SMEs and SMCs** may comply with in a simplified manner
- the AI Act's **interplay with other EU legislation**, for example the joint guidelines of the Commission and European Data Protection Board on the interplay of the AI Act and EU data protection law
- clarification of the **research exemption** (made a priority by the Commission)

Other relevant updates and changes

- Stakeholder consultation on **AI and copyright compliance** (reservation of rights, TDM)
  - *Open until 23 January*
- Launch of the **AI Office's Whistleblower tool**
  - *Reporters will be protected under EU Whistleblower Directive*
- **Uncertainty** regarding **compliance** and **deadlines**
  - *Digital Omnibus Package proposed*

3 The **Digital Omnibus Package** and its proposed amendments

New application timeline of high-risk AI rules

AI Act & Digital Omnibus Package timeline comparison

	AI Act	Digital Omnibus Package
Annex III high-risk systems	To apply from **2 August 2026**	6 months after the adoption of a decision by the Commission confirming the existence of adequate measures but no later than **2 December 2027**.
Annex I high-risk systems	To apply from **2 August 2027**	12 months after the adoption of a decision by the Commission confirming the existence adequate measures but no later than **2 August 2028**.
High-risk systems already on the market	High-risk AI systems placed on the market before 2 August 2026 → not required to comply with the AI Act obligations, unless they undergo a significant change.	Exemption period linked to the timelines indicated above.

Grace period for machine-readable content marking obligations

Article 50(2) AI Act

New timeline

- AI systems placed on the market **before 2 August 2026** - compliance required by **2 February 2027**.
- AI systems placed on the market **after 2 August 2026 - immediate compliance**.

New paragraph 4 is added to Article 111

4. Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, that have been placed on the market before 2 August 2026 shall take the necessary steps in order to comply with Article 50(2) by ***2 February 2027****.*

Removal of registration requirements

Annex III systems not deemed high-risk

Current Article 49

Registration

(…)

2. Before placing on the market or putting into service an AI system for which the provider has concluded that it is not high-risk according to Article 6(3), that provider or, where applicable, the authorised representative shall register themselves and that system in the EU database referred to in Article 71.

- Article 6(3) high-risk systems need to be registered with the EU database.

"(9) To streamline compliance and reduce the associated costs (…)."

Digital Omnibus Package

Article 49(2) is deleted.

- Registration obligations are removed.
- The requirement to maintain documentation continues to apply.

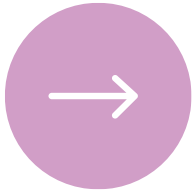
Transforming AI literacy obligation (1/2)

The EU Commission and the Member States to foster AI literacy

Current Article 4

AI Literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.



New Article 4

AI Literacy

The Commission and Member States shall encourage providers and deployers of AI systems to take measures to ensure a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, level of education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Processing SCD for bias detection and correction

Replacing Article 10(5) AI Act with new Article 4a

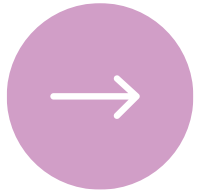
Current Article 10

Data and data governance

(…)

5. To the extent that it is **strictly necessary** for the purpose of ensuring bias detection and correction in **relation to the high-risk AI systems** in accordance with paragraph (2), points (f) and (g) of this Article (…).

(…)



New Article 4a

Processing of special categories of personal data for bias detection and mitigation

1. To the extent **necessary** to ensure bias detection and correction in relation to **high-risk AI systems** in accordance with Article 10 (2), points (f) and (g), of this Regulation (….).

2. **Paragraph 1 may apply to providers and deployers of other AI systems and models and deployers of high-risk AI systems** where necessary and proportionate if the processing occurs for the purposes set out therein and provided that the conditions set out under the safeguards set out in this paragraph.

Other key changes

Further targeted Digital Omnibus Package simplification measures

Broader use of AI regulatory sandboxes & real-world testing

Extending regulatory simplifications granted to SMEs & SMCs

Centralising oversight over a large number of AI systems built on general-purpose AI models or embedded in very large online platforms and very large search engines in the AI Office

The issuance of guidelines (in some cases instead of implementing legislation)

Offering more flexibility in post-market monitoring

Other changes clarifying the interplay between the AI Act and other EU legislation

Prospective Timeline

Under Ordinary Legislative Procedure

December 2025 plenary	Q1 - Q2 2026	Q2 - Q3 2026	Q3 - Q4 2026	Q4 2026 - Q1 2027
Proposal sent to Parliament, committees (ITRE etc.) allocated and rapporteurs appointed	Parliament & Council work in parallel to reach their respective positions	Adoption of Parliament Report and Council 'general approach'	'Trilogue' negotiations to reach consensus on final regulation	Adoption of a final agreed text by EU institutions

4 Practical steps for implementing **high-risk AI systems**

AI use cases across industries

HR/ Recruitment

- CV-Screening & Candidate Ranking
- Employee Performance Monitoring and Evaluation
- Promotion/ termination decision support

Customer and Marketing

- First-Line Customer Support
- Marketing & Sales Predictive Analytics
- Chatbots

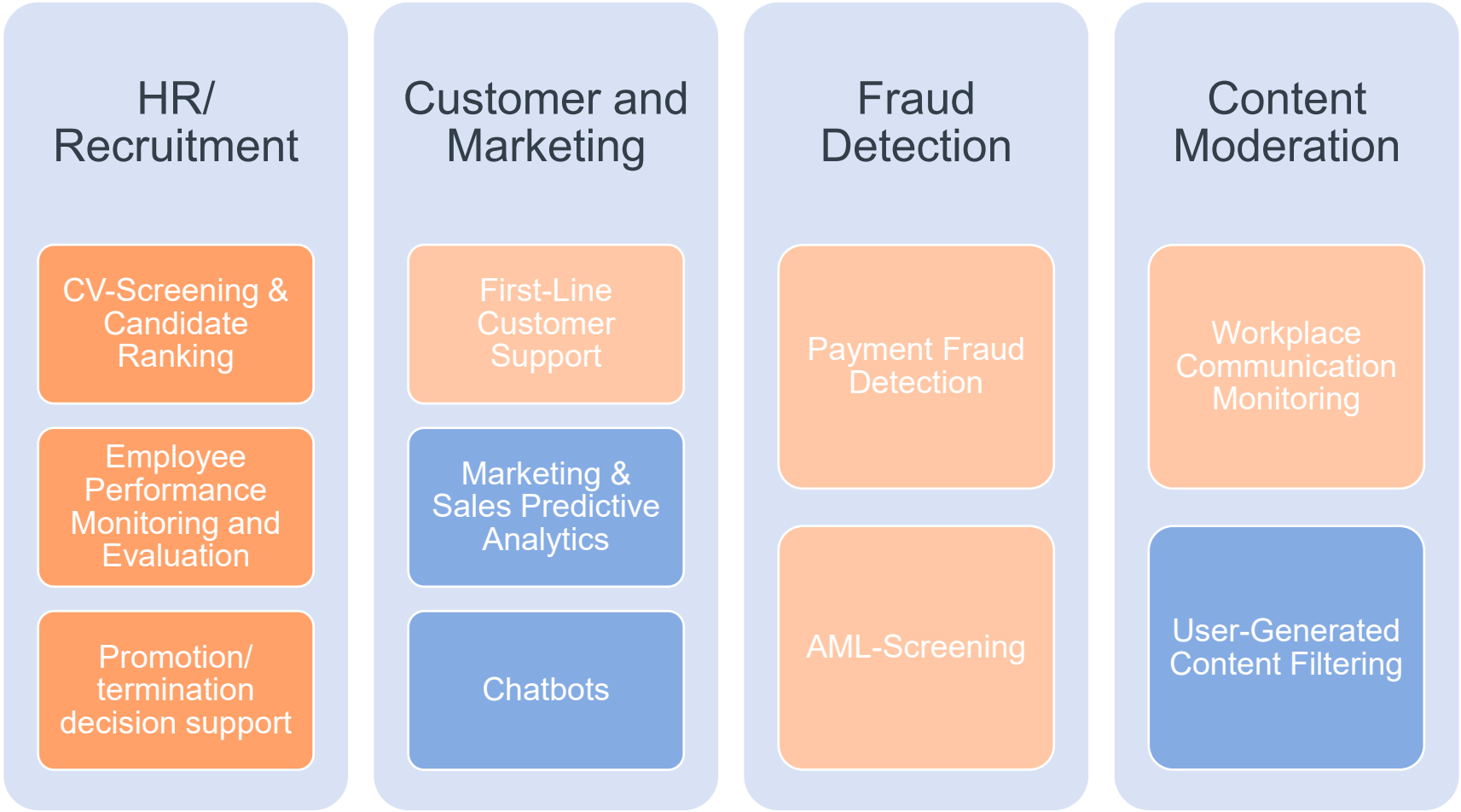
Fraud Detection

- Payment Fraud Detection
- AML-Screening

Content Moderation

- Workplace Communication Monitoring
- User-Generated Content Filtering

AI use cases across industries



Providers and deployers

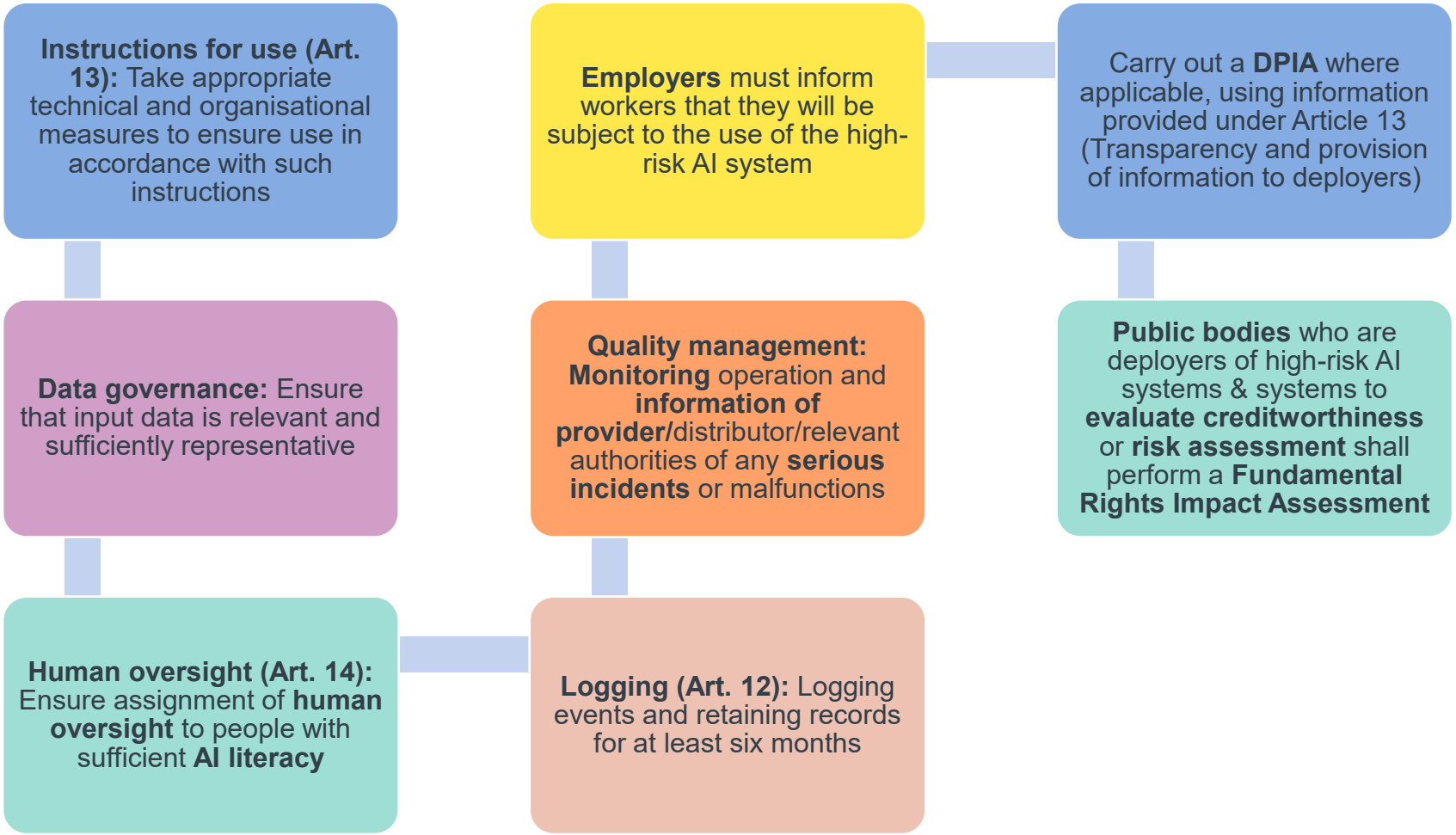
Who is in scope of the AI Act?

Providers, if			
AI system + placing on the market in the EU; regardless of where established	AI system + putting into service in the EU; regardless of where established	AI system + placing on the market/ putting into service + output used in the EU +established/ located in a third country	GPAI + putting into service in the EU; regardless of where established

Deployers, if	
AI system + use + established/ located in the EU	AI system + output used in the EU + established/ located in a third country

Also covers importers, distributors, product manufacturers and others.

Deployer obligations for high-risk AI systems



Shifting from deployer to provider

For high-risk AI systems, deployers can become a providers (Article 25)

…adds its **name or trademark** on a high-risk AI system

… makes a **substantial modification** to a high-risk AI system

…**modifies** the intended purpose of an AI system, including a general-purpose AI system, **causing it to become a high-risk system**

Provider obligations for high-risk AI systems

Article 16 AI Act

- Refers back to chapter 3, section 2 making the requirements that high-risk AI systems have to meet the provider's obligation;
- Defines further obligations for providers
- Refers forward to other obligations for providers of high-risk AI systems as defined in chapter 3, section 3 and elsewhere

All clear?

Provider obligations for high-risk AI systems

- Ensure **conformance with the following requirements** and be able to demonstrate such conformance on request:
  - Art. 9: Implementation of a risk management system to identify and address risks
  - Art. 10: Data governance and management for training, validation and testing data sets
  - Art. 11: Provide technical documentation
  - Art. 12: Allow for automatic recoding of events (record keeping)
  - Art. 13: Transparency and provision of information (instructions for use) to deployers
  - Art. 14: Ensure possibility for human oversight
  - Art. 15: Design AI system to ensure accuracy, robustness and cybersecurity
- Art. 17: Put in place a **quality management system** to ensure compliance throughout the life cycle
- Art. 18: **Documentation** keeping
- Art. 19: **Logging events** and keeping respective records
- Art. 20: Take **corrective actions** and provide information
- Art. 21: **Regulatory cooperation**
- Art. 22: **Authorised representative**
- Art. 43: Undertake **conformity assessment** prior to AI system being placed on market or put into service
- Art. 47: Draw up an **EU declaration of conformity**
- Art. 48: **Affix the CE marking** to the high-risk AI system or on its packaging etc.
- Art. 49: Comply with **registration obligations**
- Ensure **compliance with accessibility requirements** in accordance with (EU) 2016/2102 and (EU) 2019/882.
- **Provide information** re. provider on packaging/ on AI system information re provider (name, TM/ address)
- Transparency obligations

Provider obligations for high-risk AI systems

AI System Design:

- Enabling the deployer
  - Record keeping, Art. 12: Allow for automatic recoding of events
  - Instructions for use, Art.13: Transparency and information to deployers
  - Human oversight, Art. 14: Ensure it's possible
- General
  - Art.15: Design AI system to ensure accuracy, robustness and cybersecurity
  - Ensure compliance with accessibility requirements in accordance with (EU) 2016/2102, (EU) 2019/882

Policies & Procedures

- Art. 9: Risk management system to identify and address risks
- Art. 10: Data governance and management for training, validation and testing data sets
- Art. 17: Quality management system to ensure compliance throughout the life cycle
- Art. 72: Post-market monitoring system and tracking

Documentation

- Art. 11: Technical documentation
- Art. 18: Documentation keeping
- Art. 19: Logging events; keeping respective records

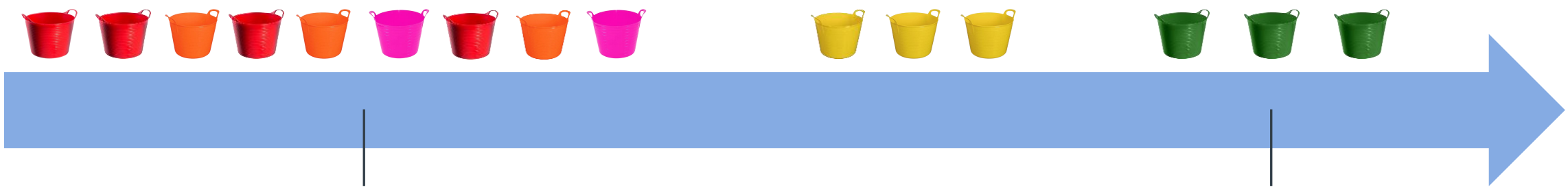
Conformity and Information

- Art.43: Undertake conformity assessment prior to AI system being placed on market/put into service
- Art. 47: Draw up an EU declaration of conformity
- Art. 48: Affix the CE marking to the high-risk AI system or on its packaging etc.
- Art. 49:Comply with registration obligations
- Provide information re. provider on packaging/ on AI system information re provider (name, TM/ address)

Accompanying tasks:

- Art. 20: Take corrective actions and provide information
- Art.21: Regulatory cooperation
- Art.22: Authorised representative
- Art.73: Reporting of serious incidents

Timeline



8 January 2026

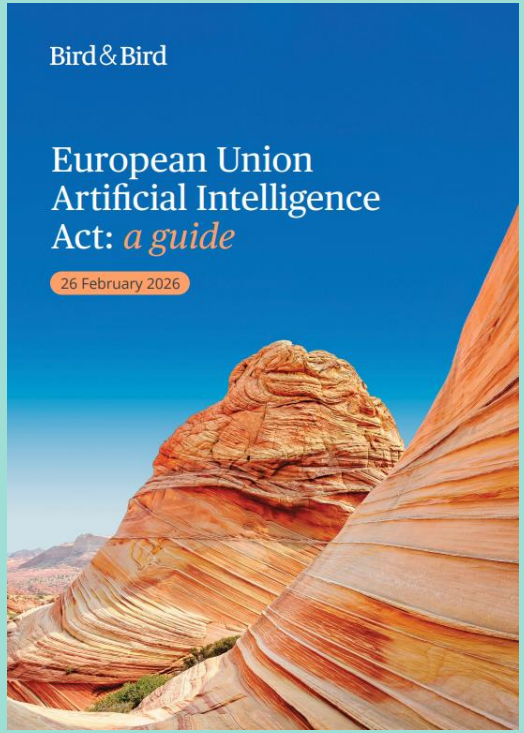
2 August 2026

2 December 2027

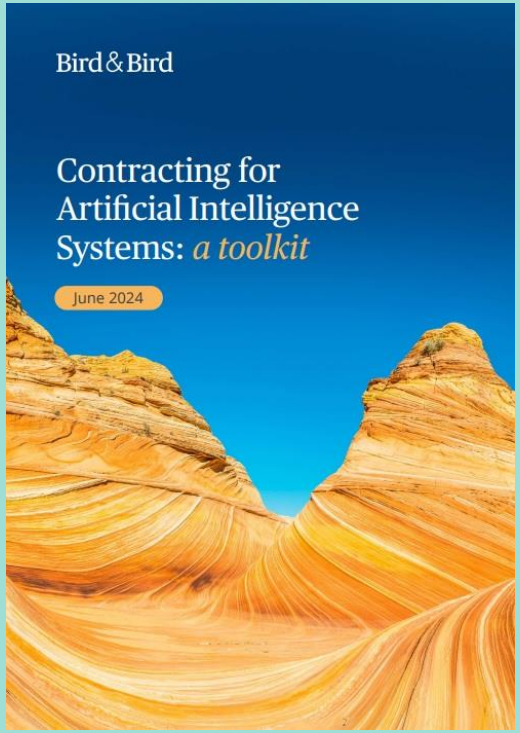
or

6 months after publication Commission

Download our *EU AI Act Guide*



Access our *Contracting for AI Toolkit*



Thank you

twobirds.com

Abu Dhabi ● Amsterdam ● Beijing ● Bratislava ● Brussels ● Budapest ● Casablanca ● Copenhagen ● Dubai ● Dublin ● Dusseldorf ● Frankfurt ● The Hague ● Hamburg ● Helsinki ● Hong Kong ● Lisbon ● London ● Lyon ● Madrid ● Milan ● Munich ● Paris ● Prague ● Riyadh ● Rome ● San Francisco ● Shanghai ● Shenzhen ● Singapore ● Stockholm ● Sydney ● Tokyo ● Warsaw