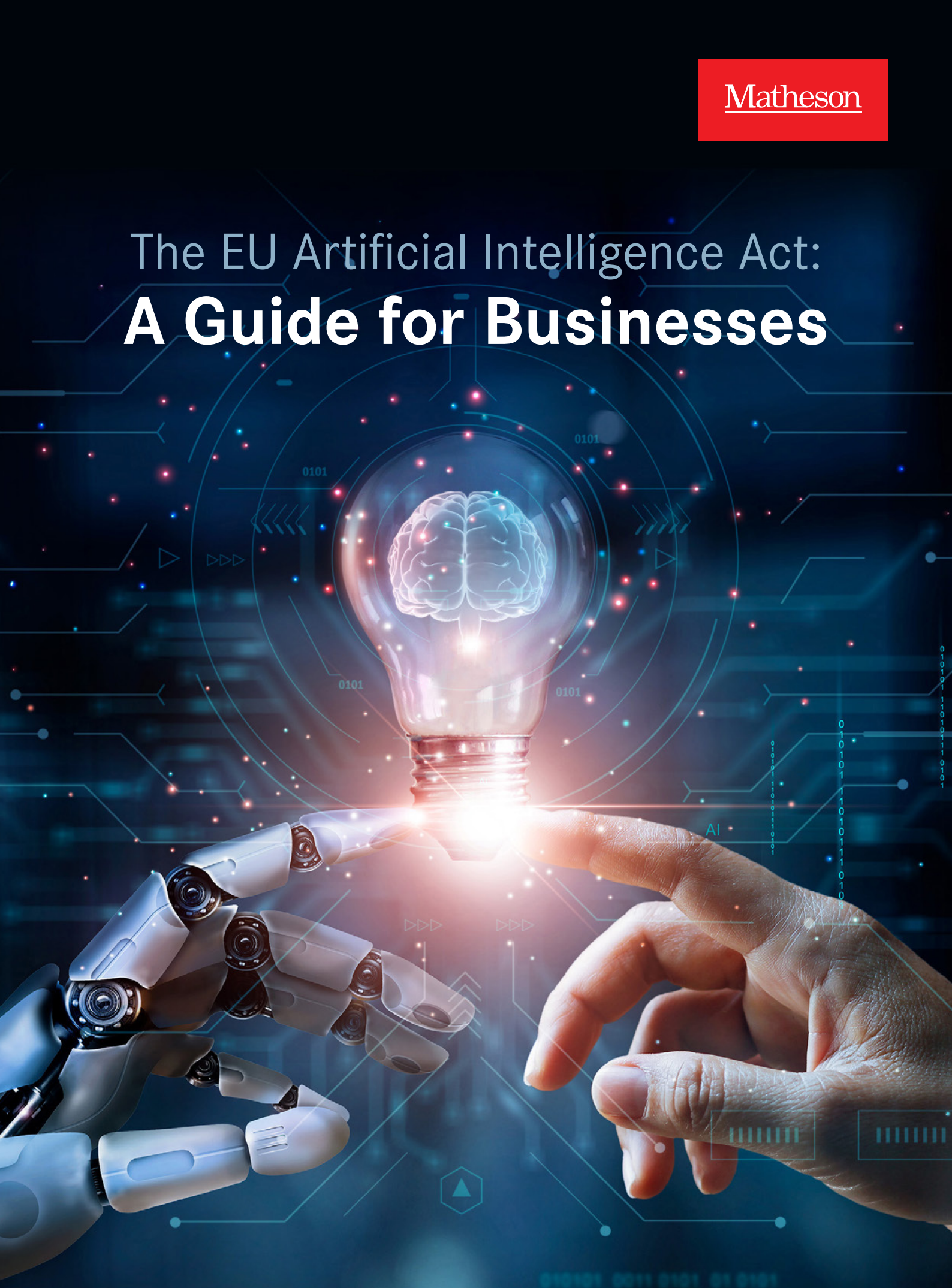
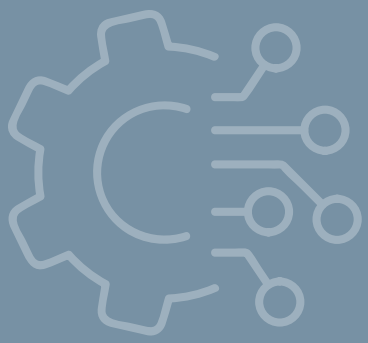
Matheson

The EU Artificial Intelligence Act:
A Guide for Businesses



Dublin Cork London New York Palo Alto San Francisco

www.matheson.com



Introduction

This Guide provides an overview of the EU Artificial Intelligence Act ("**AI Act**"), which sets out a comprehensive legal framework to regulate AI across the European Union ("**EU**"). As a European Regulation (Regulation 2024/1689), the AI Act directly applies in all 27 Member States, without the need for further national implementing legislation. We expect, however, that the Irish Government will introduce legislation providing for the appointment of the regulators responsible for enforcing the AI Act, along with their supervisory and enforcement powers. It is also due to be supplemented by delegated and implementing acts by the European Commission, guidelines, codes of practices, templates, and other supporting documentation. It will have far-reaching consequences for companies in Europe and beyond.

The purpose of the AI Act is to promote the uptake of human-centric and trustworthy AI, while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law, and environmental protection, against the harmful effects of AI systems in the EU and supporting innovation.

The AI Act lays down:

- harmonised rules for placing on the market, putting into service, and use of AI systems in the EU;
- prohibitions of certain AI practices;
- specific requirements for high-risk AI systems and obligations for operators of such systems;
- harmonised transparency rules for certain AI systems;
- harmonised rules for placing on the market of GPAI models;
- rules on market monitoring, market surveillance, governance and enforcement, including significant financial penalties for non-compliance; and
- measures to support innovation, with a particular focus on SMEs, including start-ups.

The AI Act regulates AI systems according to the level of risk associated with how they are intended to be used, with the strictest obligations being imposed on "high-risk" AI systems. The AI Act also regulates general-purpose AI ("**GPAI**") models.

The AI Act was published in the Official Journal of the EU on 12 July 2024. It entered into force on 1 August 2024, and will be fully applicable 24 months after entry into force, subject to certain exceptions. In particular, the provisions on prohibited AI systems will take effect on 2 February 2025. However, the related provisions on fines for non-compliance with these rules will, in principle, only start to apply later, on 2 August 2025 (see *Enforcement and Penalties* and *Timeline for Implementation*).

We would be happy to provide you with further information on any aspect of the AI Act on request. We look forward, to helping you to start planning and preparing for the provisions of the new AI rules coming into force.

Date of Publication: 1 October 2024.

Index

1 What AI technology is regulated by the AI Act?

In Brief

- The AI Act has broad scope, which is reflected in the definition of an "AI system". The definition is based on key characteristics of AI systems that distinguish it from simpler traditional software systems or programming approaches, and does not cover systems based on rules defined solely by natural persons to automatically execute operations.
- The AI Act also has dedicated rules for GPAI models. A prime example of a GPAI model is a large generative AI model.
- Certain AI systems are excluded from the scope of the AI Act. For example, AI systems released under free and open-source licences (subject to certain exceptions).
- The AI Act adopts a risk-based approach to the regulation of AI systems. Different rules apply to operators depending on the risk category of their AI system, and what role they are playing.

AI Systems

- The AI Act applies to an "**AI system**" which is defined 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" (Article 3(1)).
- The definition is consistent with that proposed by the Organisation of Economic Co-operation and Development ("**OECD**"). Both definitions essentially require an AI system to:
  - Be machine-based.
  - Be designed to operate with varying levels of autonomy.
  - Have the ability to infer how to generate outputs from inputs received for explicit or implicit objectives and make decisions that can influence physical or virtual environments.
  - Exhibit adaptiveness after deployment.
- Recital 12 of the AI Act notes that a key characteristic of AI systems is "their capability to infer". This capability to infer refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments.
- Although the EU legislator intended the definition of AI systems to be as broad as possible, it is not intended to cover traditional software systems or systems that are based on rules defined solely by natural persons to automatically execute operations.
- There are a number of further exclusions to the scope of the AI Act, in particular in relation to AI systems exploiting free and open-source software, subject to certain exceptions (see *What AI systems are excluded from the scope of the AI Act?*)
- The European Commission is due to develop guidelines on the practical application of the definition of an "AI system" in due course, which should provide further legal certainty on the scope of the AI Act (Article 96).

GPAI Models

- The AI Act also contains dedicated rules for "GPAI models", which are defined as a model that is "trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of performing a wide range of distinct tasks…and that can be integrated into a variety of downstream systems or applications" (Article 3(63)). A prime example of a GPAI model is a large generative AI model.
- Furthermore, the AI Act includes provisions on "GPAI systems", which are defined as AI systems based on a GPAI model, and which have the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems (Article 3(66)).

Classification of AI Systems

- The AI Act adopts a risk-based approach to the regulation of AI systems. Risk is defined as "the combination of the probability of an occurrence of harm and the severity of that harm" (Article 3(2)). Different rules apply to operators depending on the risk category of their AI system. The higher the risk of harm to society, the stricter the rules.
- The AI Act establishes four risk categories of AI systems based on the probability of an occurrence of harm and the severity of that harm:

1) **Prohibited AI practices** – These are AI systems that pose an unacceptable level of risk to the fundamental rights and values of individuals, and are strictly forbidden under the AI Act.

2) **High-Risk AI systems** – AI systems that fall under this category have a high potential to cause significant harm to the health, safety or fundamental rights of individuals. High-risk AI systems are legal, but subject to strict requirements before they can be placed on the market or put into service in the EU. These requirements aim to ensure they are trustworthy, lawful and ethical, and respect the fundamental rights and values of the EU.

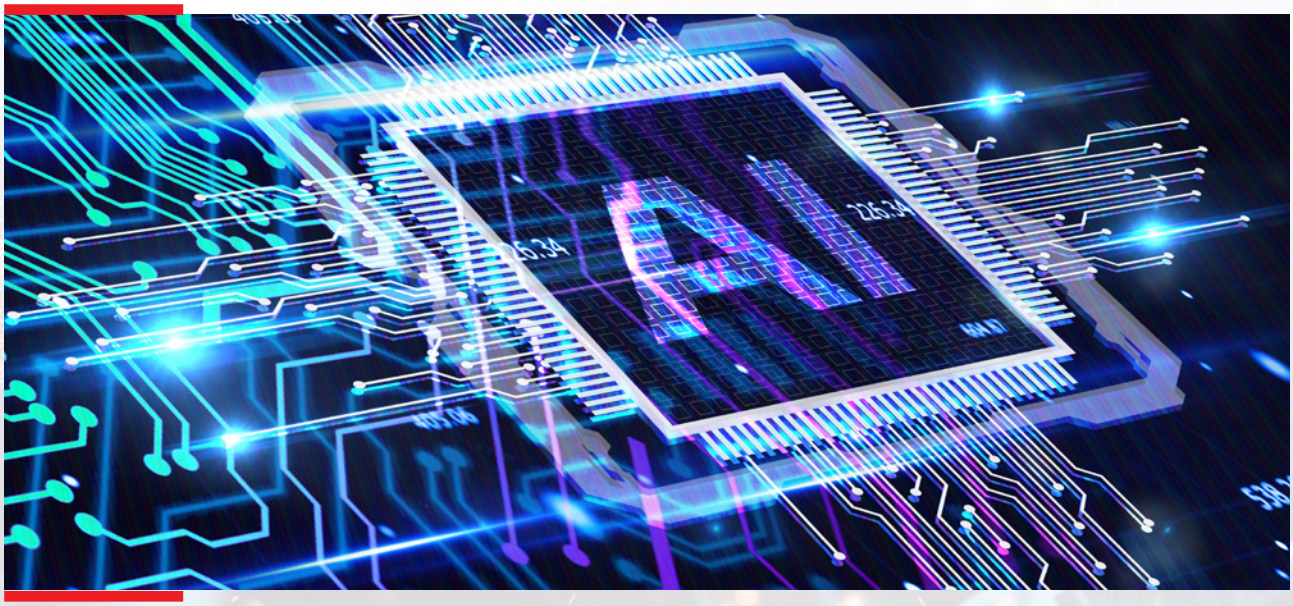
3) **Limited Risk AI systems** – These AI systems present specific transparency risks. They still need to adhere to certain safeguards, such as the transparency requirements, but they do not qualify as high-risk AI systems. An example of a limited risk AI system is an AI-powered customer service chatbot used to provide automated responses to customer questions.

4) **Minimal Risk AI systems** – These AI systems pose minimal risks to individuals' rights, safety, or societal values and are therefore subject to lighter regulatory burdens. For example, basic email filters that classify messages as spam, with a low likelihood of negative impact. Voluntarily, providers of these systems may choose to apply the requirements for trustworthy AI and adhere to voluntary codes of conduct.

- Accordingly, in determining what rules apply to operators under the AI Act, legal and compliance teams will need to consider whether the AI system they are developing or using, importing or distributing, is minimal, limited, high, or unacceptable risk. It will be important, in particular, for operators to ensure that activities which are not prohibited do not become unacceptable risk activities, therefore becoming prohibited.

- The majority of AI systems will likely present just minimal or no risk, for example, an email spam filter, and attract no obligations under the AI Act, except for the broad obligation around AI literacy which applies to all AI systems. The AI literacy obligation set out in Article 4 requires providers and deployers of AI systems to 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. This entails ensuring staff and other relevant persons have appropriate skills, knowledge, education, and training, taking account of their respective rights and obligations under the AI Act; the context the AI systems are to be used in; and the risks of using such systems.

- There are also specific rules for (i) GPAI models and for (ii) GPAI models that pose "systemic risk". GPAI models not posing systemic risks will be subject to limited requirements, such as with regard to transparency. However, providers of GPAI models that pose systemic risk will be subject to increased obligations, including performing model evaluation, assessing and mitigating possible systemic risks, ensuring an adequate level of cybersecurity protection, and reporting serious incidents to the AI Office and, as appropriate, national authorities (see *GPAI Models and Obligations*).



What AI systems are excluded from the scope of the AI Act?

- Article 2 sets out a list of specific AI systems that are excluded from the scope of the AI Act, including:
  - AI systems used exclusively for military, defence, or national security purposes (Article 2(3)).
  - AI systems used by public authorities in a third country and international organisations for compliance with international cooperation or agreements for law enforcement and judicial cooperation (Article 2(4)).
  - AI systems or AI models and output specifically developed for the sole purpose of scientific research and development (Article 2(6)).
  - Any research, testing, or development of AI systems or AI models prior to placing them on the market or putting them into service (except for testing in real world conditions) (Article 2(8)).
  - AI systems used by deployers who are natural persons for purely personal non-professional activities (Article 2(10)).
  - AI systems released under free and open-source licences, unless they are placed on the market or put into service as high-risk systems, prohibited systems, or which interact directly with a person and fall within the transparency requirements in Article 50 (Article 2(12)).
- Furthermore, for high-risk AI systems which fall within Article 6(1), relating to products covered by the EU harmonisation legislation listed in Section B of Annex I, only the obligations set out in Articles 6(1), Articles 102 to 109, Article 112 and, to a limited extent, Article 57 apply (Article 2(2)).

2 Who is regulated by the AI Act?

In Brief

- The AI Act applies to different players across the AI value chain, including providers, deployers, importers, distributors, product manufacturers, and authorised representatives (defined collectively as "operators").
- The scope of responsibilities and obligations applicable under the AI Act depends on what role the operator is playing, along with the type and intended purpose of the AI system being used.
- The AI Act has broad extra-territorial scope, and applies to certain operators not established in the EU.
- Non-EU providers of high-risk AI systems and GPAI models are required to appoint an authorised representative in the EU by written mandate.

Operators within scope of the AI Act

- The AI Act applies to different operators across the AI value chain, including providers, deployers, importers, distributors, product manufacturers and authorised representatives.
- The scope of responsibilities and obligations applicable under the AI Act depends on what role the operator is playing, along with the type and intended purpose of the AI system being used. In situations where operators act in more than one capacity at the same time, they will need to cumulatively fulfil all relevant obligations associated with those roles. We have set out further information below on the various operators whom the AI Act applies to:
  - **Providers** – A provider is any natural or legal person who develops an AI system or GPAI model, or that has them developed for them, with a view to placing it on the market or putting it into service in the EU, whether for payment or free of charge. Providers may be established or located within the EU or in a third country, if they place an AI system on the market or put it into service in the EU, or if the output produced by the AI system is used in the EU (Articles 2(1)(a) and (c) and 3(3)).
  - **Deployers** – A deployer is as any natural or legal person, public authority, agency or other body who uses an AI system (except for personal use for non-professional activities). The AI Act applies to deployers established or located within the EU. In addition, it applies to deployers of AI systems that are established or located in a third country, where the output produced by the AI system is used in the EU (Article 2(1)(b) and (c)) and 3(4)).
  - **Importers** - An importer is any natural or legal person located or established in the EU that places on the market an AI system bearing the name or trademark of a natural or legal person established in a third country (Articles 2(1)(d) and 3(6)).
  - **Distributors** – A distributor is any natural or legal person, other than the provider or importer, that makes an AI system available on the EU market (Articles 2(1)(d) and 3(7)).
  - **Product manufacturers** – Those placing on the market or putting into service an AI system in the EU together with their product and under their own name or trademark (Article 2(1)(e)).
  - **Authorised representatives** – Any natural or legal person located or established in the EU who has received or accepted a written mandate from a provider of an AI system or a GPAI model to, respectively, perform and carry out on its behalf the obligations and procedures established by the AI Act (Articles 2(1)(f) and 3(5)).
  - **Affected persons located in the EU** (Article 2(1)(g)). While the AI Act does not include a definition for "affected persons located in the EU", it is generally understood that it means individuals, and not just citizens, in the EU who might be subjected to or otherwise affected by AI systems.

Definitions

- When considering the scope of the operators' roles and application of the AI Act, it should be noted that:
  - "**placing on the market**" means the first making available of an AI system or GPAI model on the EU market (Article 3(9)).
  - "**making available on the market**" means the supply of an AI system or GPAI 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 (Article 3(10)).

- "**putting into service**" means the supply of an AI system for first use directly to the deployer or for own use in the EU for its intended purpose (Article 3(11)).
- "**intended purpose**" means 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 (Article 3(12)).

What is the territorial scope of the Act?

- The AI Act has broad extra-territorial scope, and applies to certain operators not established in the EU. The key question is the effect of the AI system on the EU, rather than where the relevant operator is necessarily based (Article 2).
- In particular, the AI Act will apply to:
  - A provider that makes an AI system or GPAI model available on the market or puts it into service in the EU, regardless of whether the provider is established or located within the EU or in a third country.
  - A provider or deployer established or located in a third country, where the output generated by the AI system is used in the EU.

Requirement to appoint an EU Authorised Representative

- Non-EU providers of high-risk AI systems and GPAI models are required to appoint an **authorised representative in the EU** by written mandate, to act as a contact point for EU regulators, and to keep copies of key compliance documentation (Articles 3(5), 22 and 54).

How does the AI Act interact with other legislation?

- The AI Act states that it does not affect the application of certain other specified legislation, including:
  - The provisions on the liability of providers of intermediary services under Chapter II of the Digital Services Act (Regulation 2022/2065) (Article 2(5)).
  - The application of the GDPR or e-Privacy Directive 2002 to the processing of personal data, without prejudice to the processing of special categories of personal data under Article 10(5) of the AI Act, and the further processing of personal data for developing certain AI systems in the public interest under Article 59 of the AI Act (Article 2(7)).
  - Rules laid down by other EU legal acts related to consumer protections and product safety (Article 2(9)).
- In certain circumstances, obligations under the AI Act may be deemed fulfilled by complying with related requirements under relevant sectoral legislation. For example, if a provider is a financial institution that is already subject to requirements regarding its internal governance or processes under EU financial services law, then the obligation to put in place a quality management system under the AI Act shall be deemed to be fulfilled, at least for part of the requirements, by complying with the rules pursuant to the relevant EU financial services law (Article 17(4)).
- In addition, the AI Act provides for a longer transition period for AI systems that qualify as high-risk AI systems due to their being products, or safety components of products, under specific sectoral legislation listed in Annex I and referred to in Article 6(1). The AI Act comes into effect on 2 August 2027 in respect of such AI systems.

3 Prohibited AI Practices

In Brief

- The AI Act prohibits certain types of AI systems. These prohibited AI systems are set out in Article 5.
- These AI systems are banned outright on the grounds that they are particularly harmful and abusive, and contradict EU values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights enshrined in the European Charter of Fundamental Rights (including the right to non-discrimination, data protection and privacy, and the rights of the child) (Recital 28).
- Non-compliance with the Article 5 prohibitions is punishable with the highest tier of administrative fines under the AI Act.

What constitutes a prohibited AI system?

- The AI Act sets out eight types of prohibited AI practices in Article 5, including:
  - **AI systems deploying subliminal, deceptive or manipulative techniques** with the objective or effect of materially distorting the behaviour of a person or group by impairing their ability to make an informed decision, in a manner that causes or is reasonably likely to cause them significant harm (Article 5(1)(a)).
  - **AI systems exploiting the vulnerabilities of a person or group**, due to their age, disability or a specific social or economic situation, with the objective or effect of materially distorting their behaviour in a manner that causes or is likely to cause them significant harm (Article 5(1)(b)).
  - **AI systems evaluating or classifying individuals or groups** based on their known, inferred or predicted personality characteristics, with the social score causing: (i) detrimental or unfavourable treatment of persons that is unjustified or disproportionate to their social behaviour, and/or (ii) detrimental or unfavourable treatment of persons in social contexts that are unrelated to the contexts in which the data was originally collected (Article 5(1)(c)). For example, AI scoring mechanisms that discriminate based on characteristics such as race, gender, or religion.
  - **AI systems assessing or predicting the risk of a person committing a criminal offence**, based solely on their profiling or on assessing their personality traits and characteristics (except where the AI system is used to support a human assessment of the involvement of a person in a criminal activity, which is based on verifiable facts) (Article 5(1)(d)).
  - **AI systems creating or expanding facial recognition databases** through the untargeted scraping of facial images from the internet or CCTV footage (Article 5(1)(e)).
  - **AI systems inferring emotions of a person in the workplace or educational institutions**, except for medical or safety reasons (i.e. monitoring the tiredness levels of a pilot) (Article 5(1)(f)).
  - **Biometric categorisation systems used to infer a person's race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation**, except any labelling or filtering of lawfully acquired biometric datasets, such as images, for law enforcement purposes (Article 5(1)(g)).
  - **Real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes**, except for (i) targeted searching for victims of abduction, trafficking or sexual exploitation, and missing persons; (ii) preventing an imminent threat to the life or physical safety of persons or a foreseeable threat of a terrorist attack; or (iii) finding persons suspected of having committed certain criminal offences (as listed in Annex II), and without prejudice to Article 9 of the GDPR (Article 5(1)(h)).
- Articles 5(2)-(7) contain further restrictions and procedural requirements which must be followed when using real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes. For example, each use of such systems must be notified to the relevant market surveillance authority and the national data protection authority in accordance with applicable national rules.

Use of real-time remote biometric identification systems for law enforcement purposes

Annex II sets out a list of criminal offences in respect of which real-time remote biometric identification systems in publicly accessible spaces are permitted. These offences, as referred to in Article 5(1)(h)(iii) include:

✔	Terrorism
✔	Trafficking in human beings
✔	Sexual exploitation of children and child pornography
✔	Illicit trafficking in narcotic drugs or psychotropic substances
✔	Illicit trafficking in weapons, munitions, or explosives
✔	Murder or grievous bodily injury
✔	Illicit trade in human organs or tissue
✔	Illicit trafficking in nuclear or radioactive materials
✔	Kidnapping, illegal restraint, or hostage-taking
✔	Crimes within the jurisdiction of the International Criminal Court
✔	Unlawful seizure of aircraft or ship
✔	Rape
✔	Environmental crime
✔	Organised or armed robbery
✔	Sabotage
✔	Participation in a criminal organisation involved in one or more of the offences listed above

Non-Compliance and Guidance

- Non-compliance with the Article 5 prohibitions is punishable with the highest tier of administrative fines under the AI Act (see *Enforcement and Penalties*).
- The European Commission is due to issue guidance on the prohibitions prior to their entry into force on **2 February 2025**.

4 High-Risk AI Systems - Classification

In Brief

- The AI Act sets out two broad categories of high-risk AI systems, including: (i) AI systems subject to EU product safety legislation listed in Annex I, and which undergo a third-party conformity assessment under that legislation; and (ii) AI systems deployed in eight specific areas listed in Annex III, including amongst others, education, employment, and access to essential public and private services.
- These AI systems are deemed to be high-risk as they could potentially create an adverse impact on people's health, safety, or fundamental rights, as protected by the EU Charter of Fundamental Rights.
- The AI Act contains a derogation in respect of high-risk AI systems which do not pose a significant risk of harm to the health, safety, or fundamental rights of natural persons, including by not materially influencing the outcome of decision-making.
- This derogation allow organisations to self-assess and determine whether their AI systems, despite being listed in Annex III, actually warrant a high-risk label.
- Even if a high-risk AI system is subject to the derogation, it must still be registered on the EU database under Article 49(2).

What is a high-risk AI system?

- The AI Act sets out a solid methodology for the classification of AI systems as "high-risk". This aims to provide legal certainty for businesses and other operators. The risk classification is based on the "intended purpose" of the AI system (as defined in Article 3(12)), in line with existing EU product safety legislation. This means the classification depends on the function performed by the AI system and on the specific purpose and modalities for which the system is used.
- There are two categories of high-risk AI systems set out in Article 6, including:
  1. AI systems intended to be used as a safety component of, or which are themselves, products covered by existing EU product safety legislation listed in Annex I, and which are required to undergo a third-party conformity assessment under that product legislation (Article 6(1)-(a) and (b)).
  2. AI systems referred to in Annex III, unless they are considered not to pose a significant risk to the health, safety, or fundamental rights of individuals, including by not materially influencing the outcome of decision-making. However, an AI system referred to in Annex III will always be considered to be high-risk where it performs profiling of individuals (Article 6(2)) (see *Derogation where High-Risk system poses no significant risk of harm)*.
- The European Commission has been tasked with maintaining a central EU database for the high-risk AI systems referred to in Annex III (Article 71) (see *Registration of high-risk AI systems on EU Database*).

What high-risk systems are listed in Annex III?

- The high-risk AI systems listed in Annex III, and referenced in Article 6(2), include use cases in the following eight areas:

1. Biometrics	a) Remote biometric identification systems (as defined in Article 3(41)) (except where it is intended to be used for biometric verification, the sole purpose of which is to confirm an individual's identity); (b) AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics; or (c) AI systems intended to be used for emotion recognition.
2. Critical infrastructure	AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating, or electricity.
3. Educational and vocational training	AI systems intended to be used to: (a) determine access or admissions to learning educational and vocational training institutions at all levels; (b) evaluate learning outcomes; (c) assess the appropriate level of education that an individual will receive or be able to access; or (d) monitor and detect prohibited behaviour of students during tests.
4. Employment	AI systems intended to be used for: (a) recruitment or selection decisions (including to analyse and filter job applications, and to evaluate candidates); or (b) making decisions affecting terms and conditions of work relationships, promotions, terminations, allocation of tasks, or to monitor and evaluate performance and behaviour.

5. Access to essential services	AI systems intended to be used: (a) by public authorities to evaluate the eligibility of individuals for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits or services; (b) to evaluate the creditworthiness of individuals except when used for the purpose of detecting financial fraud; (c) for risk assessment and pricing in relation to life and health insurance; or (d) to evaluate and classify emergency calls or to dispatch emergency services.
6. Law enforcement	AI systems intended to be used by or on behalf of law enforcement bodies: (a) to assess the risk of an individual becoming the victim of a criminal offence; (b) polygraphs or similar tools; (c) to evaluate the reliability of criminal evidence; (d) to assess the risk of an individual offending or re-offending; or (e) to profile individuals in the course of the investigation of criminal offences.
7. Migration, asylum and border control	AI systems intended to be used by or on behalf of competent public authorities: (a) as polygraphs or similar tools; (b) to assess a risk, including security or health risk, posed by an individual who intends to enter a Member State; (c) to assist with the examination of applications for asylum, visa or residence permits and any associated complaints with regard to eligibility for same; or (d) for the purpose of detecting, recognising or identifying individuals in the context of migration, asylum or border control management, with the exception of the verification of travel documents.
8. Administration of justice and democratic process	AI systems intended to be used by or on behalf of a judicial authority for: (a) researching and interpreting facts and law and in applying the law to a concrete set of facts, or (b) influencing the outcome of an election, referendum, or the voting behaviour of individuals (with the exception of AI systems used to organise, optimise or structure political campaigns from an administrative or logistical point of view).

Derogation where a high-risk system poses no significant risk of harm

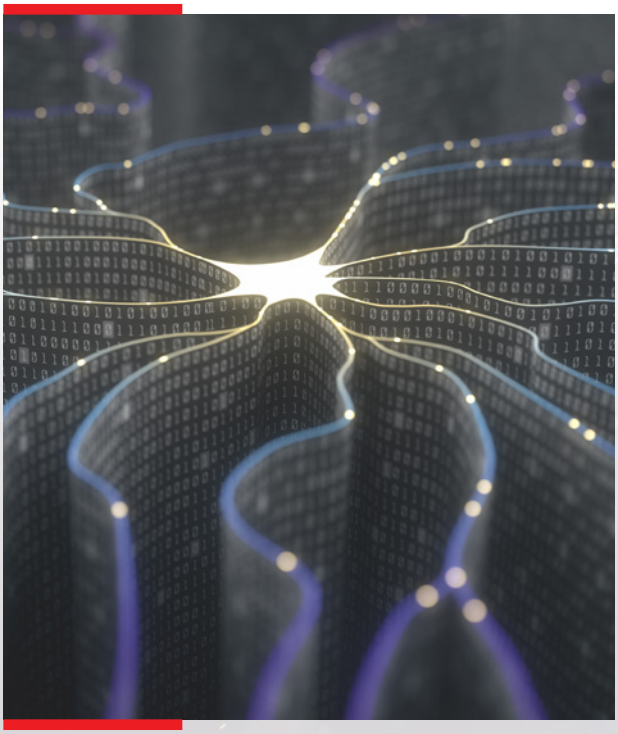
- The AI Act provides a derogation for providers where their AI system falls within an Annex III use case, but does not pose a "significant risk of harm to the health, safety, or fundamental rights of natural persons, including by not materially influencing the outcome of decision-making" (Article 6(3)).
- The AI Act sets out four examples of when this derogation applies, including 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.
  - Perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.
- Notwithstanding this derogation, an AI system referred to in Annex III will always be considered to be high-risk where the AI system performs profiling of individuals (Article 6(3)).
- Pursuant to Article 6(4), where a provider considers that the derogation applies, and their AI system is not high-risk despite falling within Annex III, the provider must:
  - Document a self-assessment as to why it is not high-risk, before the system is placed on the market or put into service, and provide a copy of the self-assessment to the national competent authorities on request.
  - Register the AI system in the central EU database in accordance with Article 49(2), and Annex VIII.

Guidelines and Voluntary Codes of Conduct

- The European Commission will, after consultation with the European Artificial Intelligence Board, and **no later than 2 February 2026**, prepare guidelines on the classification rules for high-risk AI systems, together with a list of practical examples of use cases of AI systems that are high-risk and not high-risk (Article 6(5)).
- In addition, by **2 August 2028** and every three years thereafter, the Commission is required to evaluate the impact and effectiveness of voluntary codes of conduct to foster the application of the requirements provided for high-risk AI systems in the case of AI systems other than high-risk AI systems, and possibly other additional requirements for such AI systems (Recital 174).

Applicability of AI Act to high-risk AI systems already on the market

- Operators of high-risk AI systems which have been placed on the EU market, or are subject to "significant change" in their design **on or after 2 August 2026**, and which fall within Article 6(2) and Annex III, will need to comply with the AI Act's requirements (Article 113).
- However, in order to ensure legal certainty, and avoid disruption to the market, including continuity of the use of AI systems, the AI Act applies to high-risk AI systems that are placed on the EU market **prior to 2 August 2026**, and are not intended for use by public authorities, only if, from that date, those systems are subject to a "significant change" in their design (with the exception of compliance with the rules on prohibited AI systems under Article 5, which must not be used from 2 February 2025) (Article 111(2)).
- Recital 177 suggests that the concept of "**significant change**" in this respect should be understood as equivalent in substance to the notion of "**substantial modification**", as defined in Article 3(23) of the AI Act (see *Timeline for Implementation*).



5 High-Risk AI Systems – Obligations of Providers

In Brief

- The most onerous obligations under the AI Act are imposed on providers. Section 2 (Articles 8-15) and Section 3 (Articles 16-22) of Chapter III, set out the key obligations applicable to providers of high-risk AI systems.
- Providers of high-risk AI systems are subject to a broad set of obligations, including implementing risk and quality management systems, data governance to prevent bias, documentation and record-keeping, transparency, registration, human oversight, accuracy, robustness and cybersecurity, and conformity assessments.
- Other operators in the AI supply chain should exercise caution before endeavouring to exploit the AI systems of others, as provider obligations may transfer to them, in particular where they apply their name or trade-mark to a high-risk AI system, or make a substantial modification to it, or modify the intended purpose of an AI system which has not previously been classified as high-risk.

What is the time-line for implementation of providers' obligations?

- The obligations applicable to providers (and other operators) in respect of high-risk AI systems apply from **2 August 2026** (with the exception of high-risk AI systems designed to be used as part of safety components in regulated products, which are subject to the AI Act from 2 August 2027). However, providers of high-risk AI systems are encouraged to start to comply, on a voluntary basis, with the relevant obligations under the AI Act during the transitional period (Article 113 and Recital 178) (see *Timeline for Implementation*).

What technical compliance requirements apply to providers?

- Providers of high-risk AI systems must comply with a set of technical compliance requirements set out in Articles 8-15, Section 2 of Chapter III.
- Article 8 acknowledges compliance can take into account the intended purpose of the high-risk AI system as well as the generally acknowledged state of the art on AI and AI-related technologies. Operators further down the AI supply chain have an obligation to verify compliance by those higher up the chain.
- The key **technical compliance requirements** set out in Section 2 of Chapter III, which providers of high-risk AI systems must comply with are:
- **Risk Management System (Article 9):** Establish, document and maintain a risk management system, to identify and manage risks associated with high-risk AI systems. The risk management system is not a one-off exercise that happens just before the AI system is made available on the EU market. It is a "continuous iterative process" that should be regularly reviewed and updated throughout the life-cycle of the AI system. In particular, a provider must:
  - Identify known and reasonably foreseeable risks that the AI system can pose to health, safety, or fundamental rights when used for its intended purpose and risks from possible misuse. The risks referred to here concern only those which can be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information.
  - Adopt appropriate and targeted risk management measures to minimise or eliminate risks to an acceptable level, having regard to the technical knowledge, experience, education, and training expected by the deployer, and presumable context in which the system is intended to be used. When identifying the most appropriate risk management measures, the provider should document and explain the choices made and, when relevant, involve experts and external stakeholders (Recital 65).
  - Test AI systems prior to their being placed on the EU market to ensure the most appropriate risk-management measures are put in place.
  - Consider whether the intended purpose of the AI system means the system is likely to have an adverse impact on those under 18 years of age or other vulnerable groups (i.e., whether children or vulnerable groups are likely to be exposed to the AI system's operating environment and therefore could be affected).

- **Data Quality (Article 10):** High-quality data plays a vital role in ensuring that a high-risk AI system performs as intended and safely, and it does not become a source of discrimination prohibited by EU law. Providers must develop high-risk AI systems on the basis of training, validation and testing data sets that meet the quality criteria set out in Article 10(2) to (5), whenever such data sets are used. These provisions aim to ensure that data sets used are relevant, sufficiently representative, unbiased, free of errors and complete in view of the intended purpose of the system. Where high-risk AI systems are developed without using techniques involving the training of AI models, the requirements in Article 10 apply only to the testing data sets. Providers of high-risk AI systems may exceptionally process special categories of personal data where necessary to ensure bias detection and correction, subject to complying with the GDPR and meeting all of the conditions in Article 10(5)(a)-(f). These conditions include ensuring that:
  - Use of other data, including synthetic data or anonymised data, is not sufficient to detect and correct bias.
  - The special category personal data is subject to state of the art security and privacy preserving measures, including pseudonymisation.
  - The special category personal data is subject to strict controls on access, to avoid misuse and ensure that only authorised people have access to the data.
  - The special category personal data is not transmitted, transferred, or otherwise accessed by other parties.
  - The special category personal data is deleted once the bias has been corrected or the personal data reaches the end of its retention period, whichever comes first.
  - The records of processing activities (i.e. the ROPA) includes the reasons why the processing of special category personal data is strictly necessary to detect and correct biases, and why that objective could not be achieved by processing other data.

- **Technical Documentation (Article 11):** Draw up technical documentation before the high-risk AI system is placed on the EU market or put into service, and keep such documentation up-to-date. The technical documentation must show how the AI system complies with the requirements in Section 2 of Chapter III and, at a minimum, must address the information requirements set out in Annex IV. The European Commission is required to establish a simplified technical documentation form targeted at the needs of SMEs. The information required by Annex IV is quite extensive, and includes:
  - A general description of the AI system including its intended purpose.
  - A detailed description of the elements of the AI system and the process for its development.
  - Detailed information about the monitoring, functioning and control of the AI system, including its overall expected level of accuracy.
  - A description of the appropriateness of performance metrics for the specific AI system.
  - A detailed description of the risk-management system.
  - A description of relevant changes made by the provider to the system through its life cycle.
  - A list of harmonised standards applied or other relevant standards and technical specifications applied.
  - A copy of the EU declaration of conformity.
  - A detailed description of the system in place to

evaluate the AI system performance in the post-market phase, including the post-market monitoring plan.

- **Record-Keeping (Article 12):** Design the high-risk AI system so it automatically records or logs events during its lifetime. Logs must be kept for at least six months unless otherwise provided under applicable EU or national law, in line with Article 19. The events log will enable the functioning of the AI system to be traceable for risk-identification purposes and facilitate post-market monitoring. At a minimum, each log must record: (a) the period of use of the system; (b) the reference database against which input data has been checked by the system; (c) the input data for which the search has led to a match; and (d) the name of the individual involved in human oversight activities.
- **Transparency and Provision of Information to Deployers (Article 13):** Design the high-risk AI system to ensure its operation is sufficiently transparent to deployers. The operation of the AI system must enable deployers to interpret the system's output and use it appropriately. High-risk AI systems should be accompanied with instructions for use, which must include, at a minimum, the information set out at Article 13(3)(a) to (f), including, for example, the provider's contact details, its intended purpose and the level of accuracy, robustness, and cybersecurity against which it has been tested and validated.
- **Human Oversight (Article 14):** Design and develop high-risk AI systems in such a way that they can be effectively overseen by an individual when they are in use. The purpose of human oversight is to prevent or minimise risks to the health, safety, or fundamental rights when the AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. The level of oversight must be commensurate with the risks, level of autonomy, and context of use of the AI system. In particular, the AI system must be provided to the deployer in a manner that allows the individual performing the oversight to disregard or override the output of the AI system, or to interrupt and stop its operation in a safe state. Remote biometric identification systems are subject to additional human oversight requirements given the significance of identifying an individual in this context.
- **Accuracy, Robustness and Cybersecurity (Article 15):** Design and develop high-risk AI systems in such a way that they can achieve and maintain an appropriate level of accuracy, robustness, and cybersecurity. The European Commission will develop benchmarks and methodologies to help organisations address the technical aspects of ensuring appropriate levels of accuracy and robustness. The technical solutions aimed at ensuring cybersecurity should include measures to prevent, detect, and respond to third-party attacks which try to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake (model evasion), confidentiality attacks, or model flaws.

What other obligations do providers have?

- Providers of high-risk AI systems must also comply with the key obligations set out in **Article 16** (and related obligations in Articles 17-22, Section 3 of Chapter III). These obligations include:
  - **Conformity with Technical Compliance Requirements in Section 2 of Chapter III:** Ensure, and be able to demonstrate upon request by a national competent authority, that the AI system conforms

with the technical compliance requirements set out in Articles 8-15, Section 2 of Chapter III (Articles 16(a) and (k) and Article 22).

- **Transparency:** Ensure there is information on the high-risk system, or its packaging or accompanying documentation, which indicates the provider's name, registered trade name or trade mark, and the address at which they can be contacted (Article 16(b)).
- **Quality Management System:** Implement a quality management system in compliance with Article 17. The system must be documented in the form of written policies, procedures and instructions, and show how the provider complies with the AI Act. This obligation is akin to the accountability obligation under the GDPR (Article 16(c)).
- **Record-Keeping:** Keep specified documentation for a period of 10 years after the AI system has been placed on the market or put into service. This documentation, which is specified in Article 18, includes the technical documentation, the quality management system documentation, the EU declaration of conformity, and any decisions issued by notified bodies (Articles 16(d)).
- **Retention of automatic log records:** Retain logs automatically generated by the AI system for at least six months in accordance with Article 19, and provide competent authorities with access to such logs when requested (Article 16(e) and Article 21).
- **Conformity Assessment:** Complete the conformity assessment procedure, as referred to in Article 43 (Article 16(f)) (see *Compliance and Conformity Assessment*).
- **EU Declaration of Conformity:** Draw up an EU declaration of conformity in accordance with Article 47 (Article 16(g)).
- **CE Marking:** Affix the CE marking to the AI system, or its packaging or accompanying documentation, to indicate conformity with the AI Act, in accordance with Article 48 (Article 16(h)).
- **EU Database Registration:** Register the AI system on the central EU database in accordance with Articles 49, 71, and Annex VIII (with the exception of AI systems used in connection with national critical infrastructure). Registration of critical infrastructure AI systems should be at a national level (Article 16(i)).

- **Corrective Action and Provision of Information:** Take necessary corrective actions where the AI system is not in conformity with the AI Act, or withdraw, disable, or recall it, as appropriate. Inform relevant operators and competent authorities of the non-conforming AI system in accordance with Articles 20 (Article 16(j)).
- **Accessibility:** Comply with the accessibility requirements in accordance with EU Directives 2016/2102 and 2019/882 (Article 16(l)).
- **Cooperation with competent authorities:** On request, provide relevant information to the competent authorities to demonstrate conformity with the requirements in Section 2 of Chapter III, and also give them access to the automatically generated logs of the AI system referred to in Article 12 (Article 21).
- **Appoint an Authorised Representative if not established in the EU:** Providers of high-risk AI systems established outside the EU must appoint, by written mandate, an authorised representative prior to making their systems available on the EU market (Article 22).

Transfer of Provider Obligations

- Other operators in the AI supply chain should exercise caution before endeavouring to exploit the AI systems of others, as provider obligations may transfer to them.
- Article 25(1) provides that any distributor, importer, deployer, or other third party will be considered to be a "provider" of a high-risk AI system for the purposes of the AI Act, and subject to the obligations of a provider under Article 16 in any of the following circumstances:
  - **Apply their name or trade-mark:** They apply their name or trademark to a high-risk AI system already placed on the market or put into service (without prejudice to contractual arrangements stipulating that the obligations are otherwise allocated) (Article 25(1)(a)).
  - **Make a substantial modification:** They make a "substantial modification" (as defined in Article 3(23)) to a high-risk AI system which is already on the market or put into service such that it remains high-risk (Article 25(1)(b)).
  - **Modify the intended purpose:** They modify the "intended purpose" (as defined in Article 3(12)) of an AI system, including a GPAI system, which has not been classified as high-risk, and has already been placed on the market or put into service in such a way that the AI system concerned becomes a high-risk AI system (Article 25(1)(c)).
- Where any of the circumstances set out in Article 25(1) arise, the initial provider will no longer be considered to be a provider of that specific AI system under the AI Act. The initial provider has a legal obligation to closely cooperate with new providers and make available the necessary information required for fulfilment of the obligations of providers set out in the AI Act, including compliance with the conformity assessment requirements applicable to high-risk AI systems. However, if the initial provider has clearly specified that its AI system is not to be changed into a high-risk system, it will not be subject to this cooperation obligation (Article 25(2)).
- In the case of high-risk AI systems that are safety components of products covered by the EU harmonisation legislation listed in Section A of Annex I, the product manufacturer will be considered to be the provider of the high-risk AI system, and subject to the obligations under Article 16 in either of the following circumstances:
  - the high-risk AI system is placed on the market together with the product under the name or trademark of the product manufacturer; or
  - the high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market (Article 21(3)).

Responsibilities along the AI value chain

- Any third party that supplies an AI system or tools, services, components, or processes used or integrated with a high-risk AI system must enter into a written agreement with the provider. The agreement should specify the necessary information, capabilities, technical access, and other assistance based on the generally acknowledged state of the art to enable the provider of the high-risk AI system to fully comply with its obligations under the AI Act. This requirement does not apply to third parties that make tools, services, processes, or components accessible to the public under a free and open license, except general-purpose AI models (Article 25(4)).
- The AI Office may develop and recommend voluntary model terms for contracts between providers of high-risk AI systems and third parties (Article 25(4)).

6 High-Risk AI Systems – Obligations of Other Operators

In Brief

- The AI Act imposes a comprehensive set of obligations on deployers, importers, distributors and authorized representatives to ensure the safe and compliant use of high-risk AI systems within the EU.
- The obligations imposed on these operators are set out in Section 3 of Chapter III.
- In particular, certain deployers of high-risk AI systems that fall within Annex III, will be required to carry out a Fundamental Rights Impact Assessment ("FRIA"). For example, a FRIA will be required for AI systems used to evaluate an individual's creditworthiness, or for risk assessment and pricing in relation to individuals for life and health insurance purposes.
- The AI Office will develop a template questionnaire, including through an automated tool, to assist deployers with completing a FRIA.
- To the extent that any information required to be included in the FRIA has already been included in a DPIA, the FRIA may complement the DPIA.

(A) Obligations of Deployers

What obligations do deployers have?

- Article 26 of the AI Act sets out the key obligations of deployers of high-risk AI systems. These obligations include:
  - **Complying with instructions for use:** Implement appropriate technical and organisational measures to ensure they use AI systems in accordance with the instructions for use received from the provider (Article 26(1)).
  - **Assign Human Oversight:** Assign human oversight to those who have the necessary competence, training, authority, and support to oversee the use of high-risk AI systems. Deployers remain free to organise their own resources and activities to implement the human oversight measures indicated by the providers (Article 26(2) and (3)).
  - **Input Data:** To the extent that the deployer exercises control over the input data, ensure it is relevant and sufficiently representative in light of the intended purpose of the AI system (Article 26(4)).
  - **Monitor the AI System:** Monitor the operation of the AI system on the basis of the instructions for use. Inform the provider or distributor and relevant market surveillance authority, without undue delay, where such use could present a risk to the health, safety or fundamental rights of individuals (within the meaning of Article 79(1)), and suspend use of the AI system. Where deployers identify a serious incident (as defined in Article 3(49)), they must also immediately inform the provider, and then the importer or distributor and the relevant market surveillance authority (Article 26(5)).
  - **Record-Keeping:** Retain automatically generated logs, where these are under their control, for a period of at least six months, unless provided otherwise in EU or national law, in particular data protection law (Article 26(6)).
  - **Employer obligations:** Deployers who are employers must inform workers' representatives and affected workers that they will be subject to the use of high-risk AI systems prior to such use (Article 26(7)).
  - **Public Sector Registration Obligations:** Public sector deployers must only use high-risk AI systems which are registered on the EU database and must also register their use of such systems (Article 26(8)).
  - **DPIAs:** Use the information in the instructions for use (provided under Article 13) to assist with complying with their obligation to carry out a data protection impact assessment ("**DPIA**") under Article 35 GDPR (Article 26(9)).
  - **Post-Biometric Identification:** Deployers of a high-risk AI system for post-biometric identification purposes must request authorisation from a judicial or administrative authority, except when used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence. Deployers must also submit annual reports to the relevant market surveillance and national data protection authorities on their use of post-biometric identification systems, excluding the disclosure of sensitive operational data related to law enforcement (Article 26(10)).
  - **Inform individuals of AI-assisted decision-making:** Without prejudice to Article 50, deployers

of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions about individuals must inform those individuals that they are subject to the use of such AI systems (Article 26(11)).

- **Cooperate with competent authorities:** Deployers must cooperate with relevant competent authorities in any action those authorities take in relation to the high-risk AI system (Article 26(12)).

Do all deployers need to carry out a Fundamental Rights Impact Assessment?

- Article 27(1) requires certain deployers of certain high-risk AI systems to carry out a fundamental rights impact assessment ("**FRIA**") to evaluate and mitigate the potential adverse impact of using such a system.
- Deployers are only required to carry out a FRIA for the first use of a high-risk AI system. They may, in similar cases, rely on previously conducted FRIAs or existing impact assessments carried out by the provider. Deployers have an obligation to keep their FRIAs up-to-date. (Article 27(2)).

Applicable AI Systems

- A deployer is only required to carry out a FRIA in respect of high-risk AI systems that fall under Article 6(2) and Annex III. This means, for example, that a FRAI will be required for AI systems used to evaluate an individual's creditworthiness, or for risk assessment and pricing in relation to individuals for life and health insurance purposes.
- Deployers of high-risk AI systems that are intended to be used as safety components of products or are products themselves, covered by the EU harmonisation legislation and pursuant to Article 6(1), are not required to carry out a FRIA. This is due to the fact that high-risk AI systems that fall under Article 6(1) are already separately required to undergo third-party conformity assessments before they are placed on the market or put into use pursuant to the EU harmonization legislation listed in Annex I.
- Furthermore, the obligation to complete a FRIA does not apply to deployers of high-risk AI systems intended to be used as safety components in the management and operation of critical digital infrastructure or road traffic or in the supply of water, gas, heat, or electricity.

Applicable deployers

- A FRIA must be carried out by those deployers of high-risk AI systems who are:

- Public Bodies.
- Private operators providing public services, such as education, health-care, social services, housing, and administration of services.
- Operators (such as banking or insurance entities) deploying high-risk AI systems which are intended to be used to evaluate creditworthiness of individuals or establish a credit score (with the exception of AI systems used for the purpose of detecting financial fraud), or to assess risk and pricing in relation to individuals for life or health insurance.

- In practice, many deployers using high-risk AI systems will not be required to perform a FRIA. However, they may still need to carry out a DPIA, to the extent they are acting as a controller in respect of a processing activity which is likely to result in a high-risk to the rights and freedoms of individuals, in accordance with Article 35 GDPR.

What must the FRIA cover?

- Article 27(1)(a)-(f) requires the FRIA prepared by a deployer to contain a list of mandatory information. This information includes:

✔	A description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose.
✔	The duration and frequency for which the high-risk AI system is intended to be used.
✔	The categories of individuals and groups likely to be affected by its use in the specific context at hand.
✔	The specific risks of harm likely to have an impact on the identified categories of individuals and groups.
✔	A description of the human oversight measures implemented, according to the instructions for use.
✔	The measures to be taken in case of materialisation of those risks, including internal governance arrangements and complaint mechanisms.

Template Questionnaire to assist with FRIAs

- The AI Office will develop a template questionnaire, including through an automated tool, to assist deployers with complying with their obligations regarding completion of a FRIA, and to reduce the administrative burden for deployers. Once the FRIA has been performed, the deployer must notify the market surveillance authority of its results, submitting the completed template questionnaire as part of the notification (Article 27(3) and (5)).

FRIAs and DPIAs

- It is noteworthy, that whilst there are some similarities between a DPIA and a FRIA, there are also significant differences. In particular, a DPIA specifically focuses on identifying and mitigating any risks arising in relation to personal data, whilst a FRIA assesses not only the impact on data privacy, but a wider range of fundamental rights. In addition, a FRIA, must include the mandatory information listed in Article 27(1)(a)-(f).
- To the extent that any of the information required to be contained within the FRIA, has already been included in a DPIA completed pursuant to Article 35 GDPR, the FRIA may complement the DPIA (Article 27(4)). This should reduce the administrative burden involved in compiling a FRIA, by avoiding the need to compile the same information again. However, steps should be taken to ensure that, when viewed together, the FRIA and DPIA meet the requirements of both the GDPR and AI Act.

(B) Obligations of Importers

What obligations do importers have?

- Article 23 sets out the obligations of importers of high-risk AI systems.
  - **Verify conformity:** Before placing a high-risk AI system on the EU market, importers are required to ensure that the system is in conformity with the AI Act by verifying that the provider has:
    - Completed the relevant conformity assessment (Article 23(1)(a)).
    - Drawn up the technical documentation (Article 23(1)(b)).
    - Affixed CE marking and provided the EU declaration of conformity and instructions for use (Article 23(1)(c)).
    - Appointed an authorised representative in the EU (where applicable) (Article 23(1)(d)).
  - **Non-Conformity:** Where an importer has sufficient reason to consider that a high-risk AI system is not in conformity with the AI Act, or is accompanied by falsified documentation, it must not place the system on the market until it has been brought into conformity. Where the AI system presents a risk to the health, safety or fundamental rights of persons within the meaning of Article 79(1), the importer must inform the provider, the authorised representative and the market surveillance authorities of same (Article 23(2)).
  - **Contact details:** Importers must indicate their name, address, and registered trade name or trade mark on the AI system packaging or accompanying documentation, and must co-operate with the national competent authorities on request (Article 23(3)).
  - **Technical compliance:** Importers must ensure that while a high-risk AI system is under their responsibility, storage or transport, they do not jeopardize its compliance with the technical compliance requirements set out in Articles 8-15, Section 2 of Chapter III (Article 23(4)).
  - **Record-keeping:** Importers must keep a copy of the certificate issued by the notified body (where applicable), along with the instructions for use, and the EU declaration of conformity, for 10 years after the high-risk system has been placed on the market or put into service (Article 23(5)).
  - **Provision of information to competent authorities:** Importers must provide the relevant competent authorities, upon a reasoned request, with all the necessary information and documentation to demonstrate the conformity of a high-risk AI system with the requirements set out in Articles 8-15, Section 2 of Chapter III, in a language easily understood by them (Article 23(6)).
  - **Cooperation with competent authorities:** Importers must cooperate with relevant competent authorities in any action those authorities take in relation to a high-risk AI system placed on the market by the importers, in particular to reduce and mitigate the risks posed by it (Article 23(7)).

(C) Obligations of Distributors

What obligations do distributors have?

- Article 24 sets out the obligations of distributors of high-risk AI systems, which are similar to those of importers. Distributors' obligations include:
  - **Verify Conformity:** Before placing a high-risk AI system on the market, distributors are required to ensure that the system is in conformity with the AI Act by verifying that:
    - The CE marking has been applied.
    - It is accompanied by the EU declaration of conformity, and instructions for use.
    - The provider and importer of the high-risk system have complied with their respective obligations under Article 16(b) and (c) and Article 23(3) (Article 24(1)).
  - **Non-Conformity:** Where a distributor considers, on the basis of information in its possession, that a high-risk AI system is not in conformity with the technical compliance requirements set out in Articles 8-15, Section 2 of Chapter 3, it must not place the system on the market until it has been brought into conformity. If it has already been placed on the market, the distributor must withdraw or recall it, or ensure the provider, importer or any relevant operator takes the corrective actions necessary to bring it into conformity. Where the AI system presents a risk to the health, safety or fundamental rights of persons within the meaning of Article 79(1), the distributor must immediately inform the provider or importer (as applicable) of same, and the competent

authorities, giving details of the non-compliance and any corrective actions taken (Article 24(2) and 24(4)).

- **Technical compliance:** Distributors must ensure that while a high-risk AI system is under their responsibility, storage or transport, they do not jeopardize its compliance with the technical compliance requirements set out in Articles 8-15, Section 2 of Chapter III (Article 24(3)).
- **Provision of information to competent authorities:** Distributors must provide the relevant competent authorities, upon a reasoned request, with all the necessary information and documentation to demonstrate the conformity of a high-risk AI system with the requirements set out in Articles 8-15, Section 2 of Chapter III (Article 24(5)).
- **Cooperation with competent authorities:** Distributors must cooperate with relevant competent authorities in any action those authorities take in relation to a high-risk AI system made available on the market by the distributors, in particular to reduce and mitigate the risks posed by it (Article 24(6)).

(D) Obligations of Authorised Representatives

What obligations do authorised representatives have?

- Providers of high-risk AI systems established outside the EU must appoint, by written mandate, an authorised representative prior to making their systems available on the EU market (Article 22). A copy of the written mandate must be provided to the market surveillance authorities on request.
- An authorised representative can be any natural or legal person, but must be located or established in the EU. The written mandate must empower the authorised representative to carry out the following tasks:
  - **Verify Conformity:** Verify that the EU declaration of conformity and technical documentation have been drawn up, and that an appropriate conformity assessment procedure has been completed by the provider (Article 22(3)(a)).
  - **Record-Keeping:** Retain for a period of 10 years after the high-risk AI system is placed on the market or put into service, the contact details of the provider, a copy of the EU declaration of conformity, the technical documentation, and if applicable, the certificate issued by the notified body (Article 22(3)(b)).
  - **Provision of information to competent authorities:** Provide the relevant competent authorities, upon a reasoned request, with all the necessary information and documentation to demonstrate the conformity of a high-risk AI system with the requirements set out in Articles 8-15, Section 2 of Chapter III, including access to the logs automatically generated by the system (Article 22(3)(c)).
  - **Cooperation with competent authorities:** Cooperate with relevant competent authorities in any action those authorities take in relation to a high-risk AI system, in particular to reduce and mitigate the risks posed by it (Article 22(3)(d)).
  - **Registration:** comply with the EU database registration obligations referred to in Article 49(1), or if the registration is carried out by the provider itself, ensure that the registration information submitted is correct, in particular, the name, address, and contact details of the authorised representative (Article 22(3)(e)).
- The authorised representative must terminate the mandate if it considers the provider to be acting contrary to its obligations under the AI Act. In such a case, it must immediately inform the relevant market surveillance authority and the notified body, where applicable, about the termination of the mandate and the reasons therefor (Article 22(4)).

7 GPAI Models and Obligations

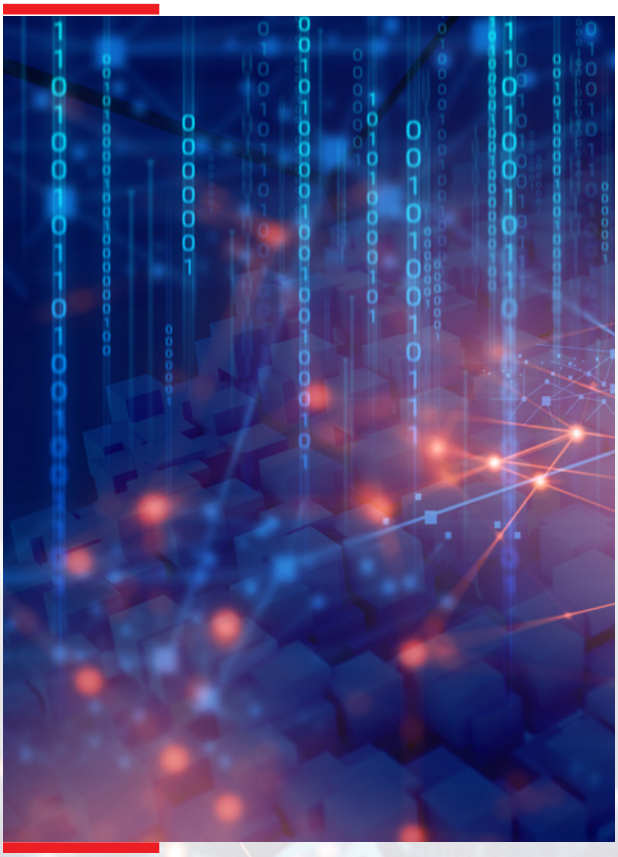
In Brief

- The AI Act contains a specific regulatory framework for providers of GPAI models, including additional requirements for those with systemic risk. There is a clear distinction between the concepts of a "GPAI model" and "GPAI system".
- The European Commission has exclusive powers regarding the supervision and enforcement of the provisions of the AI Act regarding all GPAI models (i.e. including those with systemic risk). The Commission is entrusting these tasks to the newly established AI Office.
- Providers of all GPAI models may rely on codes of practice to demonstrate compliance with their statutory obligations, until a harmonised standard is published.
- Once a harmonised standard is published, compliance with the harmonised standard will grant providers of all GPAI models a presumption of conformity, to the extent the standard covers the relevant obligations.

What is a GPAI model?

- Chapter V (Articles 51-56) of the AI Act sets out the rules governing GPAI models (as distinct from the rules on GPAI systems in Articles 25, 50 and 75). As noted by Recital 97, the notion of a GPAI Model should be clearly defined and set apart from the notion of AI systems to enable legal certainty.
- By specifying rules for GPAI models, Chapter V takes a different regulatory approach from the remainder of the AI Act, which regulates AI systems, of which GPAI systems are just one type. As discussed earlier (see *Risk-based approach to regulation*), the rules applicable to an AI system, including any GPAI systems, are determined by whether they are prohibited, high-risk, limited risk or minimal risk.
- A "GPAI Model" is defined in the AI Act as "an AI model… 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". It is noteworthy, that this definition only covers AI models that are placed on the EU market. It does not cover AI models that are used for the purpose of research, development or prototyping activities before they are placed on the market, and such activities fall outside the scope of the AI Act (Articles 3(63) and 2(8)).
- In contrast, a "GPAI system" is defined in the AI Act as "an AI system which is based on a GPAI model". When a GPAI model is integrated into or forms part of an AI system, this system should be considered a GPAI system if it has the capability to serve a variety of purposes (Article 3(66) and Recital 100).

Given that a GPAI model could be used in a high-risk case, providers will likely be subject to both high-risk and GPAI model obligations, although many of the high-risk and GPAI model obligations cover similar ground. Recital 97 confirms that when the provider of a GPAI model integrates an own GPAI model, or GPAI model that poses systemic risk, into its own AI system that is made available on the market or put into service, then the obligations in the AI Act for GPAI models will continue to apply in addition to those for AI systems.



What is a GPAI Model with systemic risk?

- Chapter V distinguishes between GPAI models with and without systemic risk. GPAI models with systemic risk are subject to stricter requirements under the AI Act due to their potential for significant harmful effects if not closely regulated.
- The AI Act establishes a methodology for the classification of GPAI models as "GPAI models with systemic risk" in the interests of legal certainty.
  - A GPAI model will be classified as a "GPAI model with systemic risk" if either of the following conditions apply:
  - It has high impact capabilities evaluated on the basis of relevant technical tools and benchmarks (Article 51(1)(a)).
  - It has been declared by the European Commission that it has high impact capabilities (either on its own initiative or following a qualified alert from the Scientific Panel), having regard to the criteria set out in Annex XIII (Article 51((1)(b)).
- Accordingly, the concept of systemic risk (as defined in Article 3(65) and in Article 51) is not assessed by a use case but by the computing power of the relevant AI model.
- The term "high impact capabilities" is not defined, but Recital 111 notes that it means "capabilities that match or exceed the capabilities recorded in the most advanced GPAI models". The AI Act states that a GPAI model will be presumed to have such "high impact capabilities" when the cumulative amount of computation used for its training is greater than 10^{25} FLOPs. (i.e. floating point operations per second) (Article 51(2)). This threshold may be amended by the European Commission in light of evolving technological developments (Article 51(3)).
- If a provider of a GPAI model meeting the classification for systemic risk considers it does not have a systemic risk, the provider can present arguments to the European Commission. Where the Commission does not agree, providers may request reassessment, at the earliest, six months after the initial designation decision (Articles 52(2)-(5)).
- The European Commission must publish a list of GPAI models with systemic risk, and keep it up-to-date (Article 52(6)).

GPAI model with systemic risk – Annex XIII criteria

- To determine whether a GPAI model has systemic risk, Annex III requires the European Commission to consider the following criteria:

✔	The number of parameters of the model
✔	The quality or size of the data set, for example measured through tokens
✔	The amount of computation used for training the model, measured in floating point operations or indicated by other variables such as estimated cost, time or energy consumption for the training.
✔	Input and output modalities of the model, such as text to text, text to image, and state of the art thresholds for determining high-impact capabilities for each modality.
✔	Benchmarks for the model capability, including level of autonomy and adaptability to learn.
✔	Whether it has high impact on the internal market due to its reach. Such high impact shall be presumed when it has been made available to at least 10,000 registered business users established in the EU.
✔	The number of registered end-users.

Obligations of providers of all GPAI Models

- Article 53 sets out the obligations of providers of all GPAI models (i.e. those GPAI models with or without systemic risk). Providers must:
  - **Keep up-to-date technical documentation:** Prepare and maintain technical documentation for the GPAI model, containing, at a minimum, the information in Annex XI (see *Mandatory information to be included in technical documentation for GPAI models*), and make it available to the AI Office and national competent authorities on request (Article 53(1)(a)).
  - **Keep up-to-date information:** Prepare, maintain, and make available information to providers of AI systems who intend to integrate the GPAI model into their AI systems. The information must: (i) enable such providers to have a good understanding of the capabilities and limitation of the GPAI model, and comply with their obligations under the AI Act, and (ii) contain the mandatory transparency information set out in Annex XII (see *Mandatory transparency information for GPAI models*) (Article 53(1)(b)).
  - **Copyright law compliance:** Put in place a policy to comply with EU copyright law and related rights, in particular, to identify a reservation of rights pursuant to Copyright Directive (EU) 2019/790 (Article 53(1)(c)).
  - **Training Transparency:** Publish a detailed summary about the content used for training the GPAI model, in line with a template provided by the AI Office (Article 53(1)(d)).
- The obligations set out above do not apply to providers of AI models that are released under a free and open source licence, given that they have, in principle, positive effects on research, innovation and competition. However, this exception does not apply to GPAI models with systemic risks (Article 53(2)).
- Providers of GPAI models may rely on codes of practice to demonstrate their compliance with the above obligations, until a harmonised standard is published (Article 53(4)).

Obligations of authorised representatives of providers of all GPAI models

- Article 54 further requires providers of GPAI models established in third countries, by written mandate, to appoint an authorised representative which is established in the EU, prior to placing a GPAI model on the EU market.
- The authorised representative must provide the AI Office with a copy of the mandate, on request. The mandate must empower the authorised representative to carry out the following tasks:
  - **Verify technical documentation:** Verify that the technical documentation containing the information specified in Annex XI has been drawn up (*see Mandatory information to be included in technical documentation for GPAI models*) and all the obligations set out in Article 53 and, where applicable, Article 55 have been fulfilled by the provider (Article 54(3)(a)).
  - **Record-Keeping:** Maintain a copy of the technical documentation and information specified in Annex XI at the disposal of the AI Office and national competent authorities, for a period of 10 years after the GPAI model has been placed on the market, and the contact details of the provider and authorised representative (Article 54(3)(b)).
  - **Provision of information to AI Office:** Provide the AI Office and competent authorities, upon reasoned request, with all the information, including technical documentation, necessary to demonstrate compliance with the obligations set out in Chapter V of the AI Act (Article 54(3)(c)).
  - **Cooperation with AI Office and competent authorities:** Cooperate with the AI Office and competent authorities, upon reasoned request, in any action they take in relation to the GPAI model, including when the model is integrated into AI systems placed on the market or put into service in the EU (Article 54(3)(d)).
- The authorised representative must terminate the mandate if it considers the provider to be acting contrary to its obligations under the AI Act. In such a case, it must immediately inform the AI Office about the termination of the mandate and the reasons therefor (Article 54(5)).
- The obligation of providers of GPAI models to appoint an authorised representative does not apply to GPAI models that are released under a free and open-source licence that allows for the access, use, modification and distribution of the model, and whose parameters are made publicly available (Article 54(6)).

Obligations of providers of GPAI models with systemic risk

- While providers of GPAI models without systemic risk only need to comply with Articles 53 and 54, providers of GPAI models with systemic risk have additional compliance obligations under Article 55. These obligations include:
  - **Perform Testing:** Perform model evaluations and testing using state of the art tools to identify and mitigate systemic risks.
  - **Risk Assessment:** Assess and mitigate possible systemic risks at EU level that may stem from the development and use of the model.
  - **Serious Incident Reporting:** Document and report, without undue delay, to the AI Office and national competent authorities any serious incidents (as defined in Article 3(49)) and possible corrective measures to address them.
  - **Cybersecurity:** Ensure an adequate level of cybersecurity protection for the model, including the physical infrastructure of the model.
- Providers of GPAI models with systemic risk may rely on codes of practice (within the meaning of Article 56) to demonstrate compliance with the obligations set out above, until a harmonised standard is published pursuant to Article 40. The AI Office launched a consultation for a first Code of Practice for GPAI models on 30 July 2024. The AI Act requires codes of practice to be ready at least **by 2 May 2025** (Article 56(9)).
- Once a harmonised standard is published and assessed as suitable to cover the relevant obligations by the AI Office, compliance with a harmonised standard will grant providers a presumption of conformity. Providers of GPAI models with systemic risks who do not adhere to an approved code of practice or do not comply with a European harmonised standard must demonstrate alternative adequate means of compliance for assessment by the Commission (Article 55(2)).

Mandatory information to be included in technical documentation for GPAI models

Annex XI sets out the information to be included in technical documentation provided by all providers of GPAI models, as referred to in Article 53(1)(a). We have set out a summary of this information below.

All GPAI Models (with or without systemic risk)

- **A general description of the GPAI model, including:**

✔	The tasks that the model is intended to perform and the type and nature of AI systems in which it can be integrated.
✔	The acceptable use policies applicable.
✔	The date of release and methods of distribution.
✔	The architecture and number of parameters.
✔	The modality (e.g. text or image), and format of inputs and outputs.
✔	The license.

- **Relevant information about the process for the development, including:**

✔	The technical means required to integrate the GPAI model in AI systems (e.g. instructions for use, infrastructure and tools).
✔	The design specifications of the model and training process, including training methodologies and techniques. The key design choices, including the rationale and assumptions made, what the model is designed to optimize, and the relevance of the different parameters.
✔	Information on the data used for training, testing and validation, when applicable, including the type and provenance of data and curation methodologies (e.g. cleaning and filtering); the number of data points, their scope and main characteristics; how the data was obtained and selected; as well as all other measures to detect the unsuitability of data sources and methods to detect identifiable biases, where applicable.
✔	The computational resources used to train the model (e.g. number of floating point operations), training time and other relevant details related to the training.

✔	The known or estimated energy consumption of the model. When the energy consumption of the model is unknown, the energy consumption may be based on information about computational resources used.

GPAI Models with systemic risk

- **Additional information to be provided by providers of GPAI models with systemic risk includes:**

✔	A detailed description of the evaluation strategies, including evaluation results, based on available public evaluation protocols and tools or other evaluation methodologies. Evaluation strategies shall include evaluation criteria, metrics and methods for identifying limitations.
✔	A detailed description, where applicable, of the measures implemented to conduct internal and/or external adversarial testing (e.g. red teaming), model adaptations, including alignment and fine tuning.
✔	Where applicable, a detailed description of the system architecture that explains how software components build or feed into each other and integrate into the overall processing.

Mandatory transparency information for GPAI models

Annex XII sets out the transparency information to be included in technical documentation provided by providers of GPAI models to downstream providers (as defined in Article 3(68)) that integrate the model into their AI system, as referred to in Article 53(1)(b). We have set out a summary of this information below.

All GPAI models (with or without systemic risk)

- **A general description of the GPAI model including:**

✔	The tasks that the model is intended to perform and the type and nature of AI systems into which it can be integrated.
✔	The acceptable-use policies applicable.
✔	The date of release and methods of distribution.
✔	How the model interacts, or can be used to interact, with hardware or software that is not part of the model itself, where applicable.
✔	The versions of relevant software related to the use of the GPAI model, when applicable.
✔	The architecture and number of parameters.
✔	The modality (e.g. text or image), and format of inputs and outputs.
✔	The license for the model.

- **A description of the elements of the model and of the process for its development, including:**

✔	The technical means required to integrate the GPAI model into AI systems (e.g. instructions for use, infrastructure and tools).
✔	The modality (e.g. text or image), and format of the inputs and outputs and their maximum size (e.g. context or window length).
✔	Information on the data used for training, testing and validation, where applicable, including the type and provenance of data and curation methodologies.

Supervision and enforcement of providers of all GPAI models

- The European Commission will have exclusive powers to supervise and enforce Chapter V, Articles 51-56 regarding the obligations of providers of GPAI models. The Commission will entrust the implementation of these tasks to the AI Office (Article 88).
- The AI Office has broad powers to take all "necessary actions" to monitor and enforce compliance by providers of GPAI models, including their adherence to approved codes of practice (Article 89(1)). It should be able to investigate possible infringements of the rules on providers of GPAI models both on its own initiative, following the results of its monitoring activities, or upon request from market surveillance authorities (Recital 162).
- Downstream providers in the AI supply chain will have the right to lodge complaints alleging an infringement of the AI Act by the provider of the GPAI model (Article 89(2)).
- The Scientific Panel may also provide a qualified alert to the AI Office where it has reason to suspect that:
  - the GPAI model poses concrete identifiable risk at EU level; or
  - the GPAI model meets the classification requirements for a GPAI model with systemic risk (Article 90(1)).

Investigation powers of Commission regarding GPAI models

- The European Commission may request the provider of a GPAI model to provide any documentation that is necessary for the purpose of assessing the provider's compliance with the AI Act. Before requesting such information, the AI Office may enter into a structured dialogue with the provider of the GPAI model (Article 91(1)-(2)).
- The AI Office, after consulting with the European Artificial Intelligence Board, may conduct an evaluation of the GPAI model concerned to:
  - assess compliance of the provider with its obligations under the AI Act, where the information gathered pursuant to Article 91 is insufficient; or
  - to investigate systemic risks at EU level of GPAI models with systemic risk, in particular any qualified alert from the Scientific Panel in accordance with Article 90(1).

  For the purposes of carrying out this evaluation, the Commission may request access to the GPAI model concerned through APIs or further appropriate technical means and tools, including source code.

Corrective powers of Commission regarding GPAI models

- Where necessary and appropriate, the European Commission may request providers to take certain corrective measures, including:
  - Measures to comply with the obligations set out in Articles 53 and 54.
  - Implement mitigation measures, where the evaluation carried out in accordance with Article 92 has given rise to serious and substantiated concern of a systemic risk at EU level.
  - Restrict the making available on the market, withdraw or recall the model.
- Before a measure is requested, the AI Office may initiate a structured dialogue with the provider of the GPAI model. If the provider proceeds to offer commitments to implement certain mitigation measures to address a systemic risk, the Commission may declare that there are no further grounds for action (Articles 93(1)-(3)).

Procedural rights of providers of GPAI models

- Article 94 provides that Article 18 of the Regulation (EU) 2019/1020 (the "**EU Market Surveillance Regulation**") (which sets out certain procedural rights of economic operators following a regulatory decision) shall apply to providers of GPAI models, without prejudice to the more specific procedural rights provided for in the AI Act.

When do the rules for providers of GPAI models come into effect?

- The rules for providers of GPAI models come into effect in two phases.
- Providers of GPAI models placed on the EU market before 2 August 2025 have until 2 August 2027 to comply. However, providers of all other GPAI model providers (i.e. those placed on the EU market on or after 2 August 2025) must comply with the AI Act's rules by 2 August 2025 (see *Timeline for Implementation*).

8 Transparency Obligations

In Brief

- Certain AI systems intended to interact with individuals or to generate content may pose specific risks of impersonation or deception, irrespective of whether they qualify as high-risk AI systems or not. Providers and deployers of such AI systems are subject to transparency obligations. For example, users must be informed that they are interacting with an AI system, such as a chatbot.
- Exceptions and specificities apply such as in regard to law enforcement, or in regard to deep fakes created in connection with artistic or satirical works.

Who do the transparency obligations apply to?

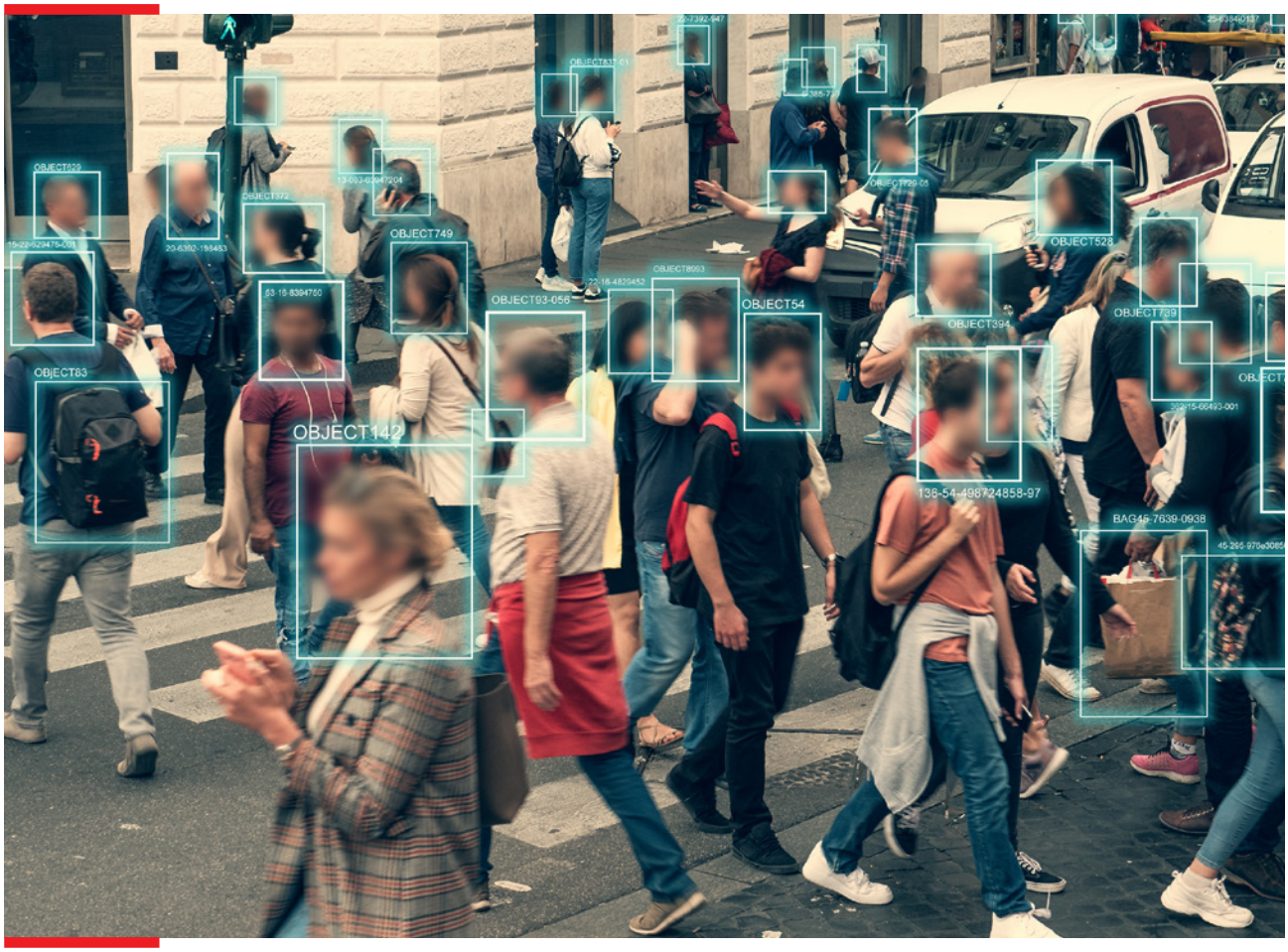
- Article 50 sets out transparency obligations which apply to providers and deployers of AI systems, which are intended to interact with individuals or which generate content viewed by individuals.
- Recital 132 indicates that the transparency obligations apply irrespective of whether the AI system qualifies as high-risk or not. Accordingly, the transparency obligations apply to limited risk, high-risk or GPAI systems that interact with individuals or generate content that may pose specific risks of impersonation or deception (pursuant to Articles 50(1)-(4), and as discussed further below).
- Providers and deployers must comply with their respective transparency obligations, at the latest, at the time of an individual's first interaction with, or exposure to the AI system. These transparency obligations apply without prejudice to other transparency obligations set down in EU or national law, such as under the GDPR.

Transparency obligations of providers

- **AI systems directly interacting with individuals:** Providers of AI systems that directly interact with an individual must ensure that the AI system informs the individual that they are interacting with an AI system, unless this is obvious, taking into account the circumstances and context of use. Such AI systems would include a chatbot handling customer inquiries. This obligation does not apply to AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences, unless those systems are available for the public to report a criminal offence (Article 50(1)).
- **AI systems generating synthetic content viewed by individuals:** Providers of AI systems, including GPAI systems, which generate synthetic audio, image, video or text content must ensure that the outputs of the AI system are marked and detectable as artificially generated or manipulated (such as through a watermark etc.). This obligation does not apply to AI systems which perform an assistive function for standard editing or do not substantially alter the input data provided by the deployer, or where authorised by law to detect, prevent, investigate or prosecute criminal offences (Article 50(2)).

Transparency obligations of deployers

- **Emotion Recognition or Biometric Categorisation:** Deployers of an emotion recognition system or a biometric categorisation system (as defined in Articles 3(39) and 3(40) respectively) must inform individuals of the operation of the system, and process the personal data in accordance with the GDPR, the Law Enforcement Directive, and EU Regulation 2018/1725, as applicable. This obligation does not apply where use of the AI system is authorised by law to detect, prevent or investigate criminal offences (Article 50(3)).



- **Deep fakes:** Deployers of an AI system that generates or manipulates image, audio or video content which is a deep fake (as defined in Article 3(60)), must disclose that the content has been artificially generated or manipulated. For example, a video that simulates a person saying things they never said in real life. This obligation does not apply where use of the AI system is authorised by law to detect, prevent or investigate criminal offences. In circumstances where the content forms part of an evidently artistic, satirical or fictional work or programme, this obligation is limited to disclosure of the existence of such generated or manipulated content in a manner that does not hamper the display or enjoyment of the work (Article 50(4)).
- **AI system generating synthetic text published to inform the public on matters of public interest:** Deployers of an AI system that generates or manipulates text published to inform the public about matters of public interest must disclose that the text has been artificially generated or manipulated. For example, AI-generated news articles or stories that may be mistaken for human-written content. This obligation does not apply where use of the AI system is authorised by law to detect, prevent or investigate criminal offences, or where the AI-generated content has undergone a process of human review or editorial control and where a natural or legal person holds editorial responsibility for publication of the content (Article 50(4)).

Are there any guidelines on the transparency obligations?

- The AI Office will issue guidelines to assist providers and deployers to comply with their transparency obligations under Article 50. The transparency obligations apply to providers and deployers from **2 August 2026** (i.e. two years after the entry into force of the AI Act). The AI Office will also encourage and facilitate the development of Codes of Practice at EU level to streamline the effective implementation of the obligations related to the detection and labelling of artificially generated or manipulated content (Articles 96(1) and 50(7)).

9 Conformity and Compliance Assessments

In Brief

- The AI Act contains specific rules and presumptions on conformity of high-risk AI systems (Articles 40-49).
- Before placing a high-risk AI system on the EU market or otherwise putting it into service, providers must complete the relevant conformity assessment procedure, including either (i) the self-assessment conformity procedure or (ii) the conformity assessment by a notified body. For most conformity assessments, in particular those listed in Annex III (2) to (8), providers can follow the self-assessment conformity procedure.
- Providers of high-risk AI systems must also draw up an EU declaration of conformity and affix a CE marking to their AI systems or its packaging to indicate conformity with the AI Act.
- In addition, providers of certain high-risk AI systems must register the system on the EU database.

Evidencing conformity

- Article 43(1) requires providers of high-risk AI systems to complete either:
  a. The self-assessment conformity procedure (i.e. the conformity assessment procedure based on internal control) as set out in Annex VI; or
  b. The conformity assessment by a notified body as set out in Annex VII.

  (See *Self-Assessment Conformity Procedure* and *Conformity Assessment by a Notified Body*).
- Most conformity assessments can be completed by the provider using the self-assessment conformity procedure, as set out in Annex VI.
- For high-risk AI systems covered by EU harmonisation legislation listed in Section A of Annex I, the provider must follow the relevant conformity assessment procedure required by those legal acts. The requirements in Articles 8-15, Section 2 of Chapter III shall also apply to those high-risk AI systems, and shall be part of that assessment. In addition, certain parts of Annex VII shall also apply (Article 43(3)).
- High-risk AI systems that have already been subject to a conformity assessment procedure must undergo a new conformity assessment procedure in the event of a "substantial modification", regardless of whether the modified system is intended to be further distributed or continues to be used by the current deployer (Article 43(4)).
- "Substantial modification" is defined in Article 3(23) as any "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".
- Each Member State is required to designate or establish at least one notifying authority, which will be responsible for setting up and carrying out the necessary procedures for the assessment, designation, and notification of conformity assessment bodies and for their monitoring. The AI Act includes provisions on the application process and requirements for conformity assessment bodies (Articles 28-39).

Self-assessment conformity procedure

- For high-risk systems referred to in Annex III (2)-(8), providers can follow the self-assessment conformity procedure.
- The self-assessment conformity procedure, as set out in **Annex VI**, requires providers of high-risk AI systems to:

✔	Verify that the established quality management system is in compliance with Article 17.
✔	Ensure the technical documentation is in compliance with the Articles 8-15, Section 2 of Chapter III.
✔	Verify that the design and development process of the AI system and its post-market monitoring are consistent with the technical documentation.

- Reliance on self-assessment will depend heavily on the availability of harmonised standards (see *Harmonised Standards* below). Where self-assessment is not possible, the provider must undergo assessment using

a notified body, in line with the process set out in Annex VII.

Conformity assessment by notified body

- Providers of high-risk AI systems must follow the conformity assessment procedure involving a notified body as set out in Annex VII (rather than the self-assessment conformity procedure) where:
  - Harmonised standards do not exist, and there are no common specifications available.
  - The provider has not applied, or has only applied part of, the harmonised standard.
  - The common specifications exist, but the provider has not applied them.
  - One or more of the harmonised standards contains a restriction.
- For the purposes of this conformity assessment procedure, the provider may choose any of the notified bodies. However, where the high-risk AI system is intended to be put into service by law enforcement, immigration or asylum authorities or other EU bodies, the market surveillance authority shall act as notified body.

Derogation from conformity assessment procedure

- A market surveillance authority may authorise the placing on the market or putting into service of specific high-risk AI systems, pending completion of a conformity assessment, for exceptional reasons of public security or the protection of life or health of persons, environmental protection or the protection of key industrial and infrastructural assets. The authorisation will be for a limited period while the conformity assessment is completed (Article 46(1)). Where the European Commission considers the authorisation is unjustified, it will be withdrawn by the market surveillance authority of the Member State concerned (Article 46(6)).
- For high-risk AI systems related to products covered by EU harmonisation legislation listed in section A of Annex I, only the derogations from the conformity assessment established in that EU harmonisation legislation will apply (Article 46(7)).

Harmonised standards

- There is a "presumption of conformity" for high-risk AI systems or GPAI models developed in conformity with harmonised standards (Article 40(1)). The European Commission is required (in accordance with Article 10 of the EU Standardisation Regulation No.1025/2012) to request standardisation organisations to issue harmonised standards covering the technical compliance requirements applicable to providers of high-risk AI systems under Chapter III, Section 2, Articles 8-15, and the obligations applicable to GPAI models under Articles 53-55.
- In May 2023, the European Commission reportedly mandated the European standardisation organisations, CEN and CENELEC, to develop harmonised standards for these high-risk requirements. The mandate has since been amended, to align with the final text of the AI Act.
- The European Commission has stated that the standardisation organisations will have until the end of April 2025 to develop and publish these standards. The European Commission will then evaluate and possibly endorse the standards, which will be published in the EU's Official Journal.

Common specifications

- If harmonised standards are not completed in time, or do not comply with the European Commission's request, the Commission may designate suitable existing international standards to apply in the interim. Compliance with the common specifications will also confer a "presumption of conformity" with the AI Act requirements in Articles 8-15, Section 2 of Chapter III, and the obligations applicable to GPAI models under Articles 53-55, to the extent such common specifications cover those requirements (Article 41(1)).
- Where providers of high-risk AI systems or GPAI models do not comply with the common specifications, they must duly justify that they have adopted technical solutions that meet the requirements set out in Articles 8-15 or, as applicable, Articles 53-55 to at least an equivalent level (Article 41(5)).

Conformity certificates

- On successful completion of a conformity assessment by a notified body, that body will issue a certificate to the provider. The certificate will be valid for the period they indicate, which must not exceed a period of five years for AI systems covered by Annex I, and four years for AI systems covered by Annex III. The provider may, however, request the certificate to be extended, subject to reassessment (Article 44(1)).

- A notified body may suspend or withdraw a certificate or impose restrictions on it, if it finds that an AI system no longer meets the requirements set out in Articles 8-15, Section 2 of Chapter III (Article 44(2)). Decisions of notified bodies, including on conformity certificates issued, may be appealed (Article 44(3)).

EU declaration of conformity

- Article 47 requires providers of high-risk AI systems to draw up a written machine readable, physical or electronically signed EU declaration of conformity for each high-risk AI system. The declaration must be kept for 10 years after the high-risk AI system has been placed on the market or put into service, and a copy must be submitted to the relevant national competent authorities on request.
- The EU declaration of conformity shall contain the information set out in Annex V, including, in particular, that the high-risk AI system is in conformity with the requirements set out in the AI Act. Where the AI system involves the processing of personal data, the declaration of conformity must further state that the system complies with applicable EU data protection law. It must be kept up-to-date, and translated into a language that can be easily understood by the national competent authorities of the Member States in which the high-risk system is placed on the market or made available.
- Where high-risk AI systems are subject to other EU harmonisation legislation which also requires an EU declaration of conformity, a single EU declaration of conformity may be drawn up.

Annex V: EU Declaration of Conformity information

- Annex V requires an EU declaration of conformity issued by the provider to contain the following information:

✔	AI system name, type and any additional unambiguous reference enabling identification and traceability of the AI system.
✔	The name and address of the provider or their authorised representative (where applicable).
✔	A statement that the EU declaration of conformity is issued under the sole responsibility of the provider.
✔	A statement that the AI system is in conformity with the AI Act, and any other EU law requiring the issuing of the EU declaration of conformity.
✔	Where an AI system requires the processing of personal data, a statement that the AI system complies with the GDPR, EU Regulation 2018/1725 or the Law Enforcement Directive (as applicable).
✔	References to any relevant harmonised standards or common specifications in relation to which conformity is declared.
✔	The name and identification number of the notified body, a description of the conformity assessment procedure performed, and the conformity certificate issued.
✔	The place and date of issue of the declaration, and the name and function of the person who signed it.

Affixing CE marking

- Providers of high-risk AI systems must affix CE marking to their AI systems or, where that is not possible, to its packaging or accompanying documentation, to indicate conformity with the AI Act (Articles 16(h) and 48).
- A digital CE marking may be used, if it can be easily accessed via the interface from which the AI system is accessed, or via an easily accessible machine-readable code or other electronic means.
- If conformity was assessed by a notified body, the CE marking should be followed by the identification number of that notified body. The notified body should affix the identification number itself, or the provider or the provider's authorised representative may affix it on the notified body's instructions.

Registration of high-risk AI systems on EU Database

- Before placing on the market or putting into service a high-risk AI system listed in Annex III (with the exception of high-risk AI systems forming national critical infrastructure listed in Annex III(2)), providers or their authorised representatives (where applicable), must register themselves and their systems in the EU database (Articles 16(i) and 49(1)). Registration of critical infrastructure AI systems listed in Annex III(2) should be at a national level (Article 49(5)).
- The AI Act also requires providers to register AI systems which they have concluded are not high-risk in accordance with Article 6(3) (see *Derogation where High-Risk system poses no significant risk of harm*). It further requires registration by deployers of high-risk AI systems who are public authorities, agencies or persons acting on their behalf to register (Articles 49(2) and 49(3)).
- The EU database serves as a tool to promote transparency and accountability of providers and deployers of high-risk AI systems through public oversight. The EU database will serve as a central repository for detailed information about high-risk AI systems that fall within the scope of 6(2).
- The details which must be registered in the EU database are set out in Annex VIII. The data listed in Sections A and B of Annex VIII shall be entered into the EU database by the provider or the authorised representative (where applicable) (Article 71(2)). The data listed in Section C of Annex VIII shall be entered into the EU database by the deployer who is, or who acts on behalf of, a public authority, agency, or body (Article 71(3)).
- For high-risk AI systems in the areas of law enforcement, migration, asylum and border control management, registration details shall be kept in a secure non-public section of the EU database, and shall include more limited information. Only the European Commission and national authorities shall have access to the restricted sections of the EU database (Article 49(4)).

10 Governance

In Brief

- The AI Act establishes a two-tiered governance system. National authorities are responsible for overseeing and enforcing rules for AI systems. Meanwhile at EU level, the AI Office established within the European Commission is responsible for governing and sanctioning providers of all GPAI models.
- Chapter VII, Articles 64-69 set out the roles and functions of various official bodies established by the European Commission to oversee the implementation of the AI Act at EU level. These bodies include: the European Artificial Intelligence Board, and the AI Office, along with two new advisory bodies, the Scientific Panel and the Advisory Forum.
- The new advisory bodies will offer valuable insights from interdisciplinary scientific communities and stakeholders, informing decision-making and ensuring a balanced approach to AI development.

Who is responsible for governance at EU level?

The AI Office

- The European Commission decision establishing the AI Office was published on 24 January 2024. The AI Office, which will sit within the Directorate-General for Communication Networks, Content and Technology in the European Commission.
- The AI Office will play a key role in implementing the AI Act by supporting the governance bodies in Member States in carrying out their tasks.
- It will also enforce the rules for GPAI models. This is underpinned by the powers given to the European Commission by the AI Act, including the ability to conduct evaluations of GPAI models, request information and measures from model providers, and apply sanctions. In addition, it will develop guidance and codes of practice to help organisations understand their new obligations.
- In addition, the AI Office may develop and recommend voluntary model terms for contracts between providers of high-risk AI systems and third parties that supply tools, services, components, or processes that are used for or integrated into high-risk AI systems (Article 25(4)).

The European Artificial Intelligence Board

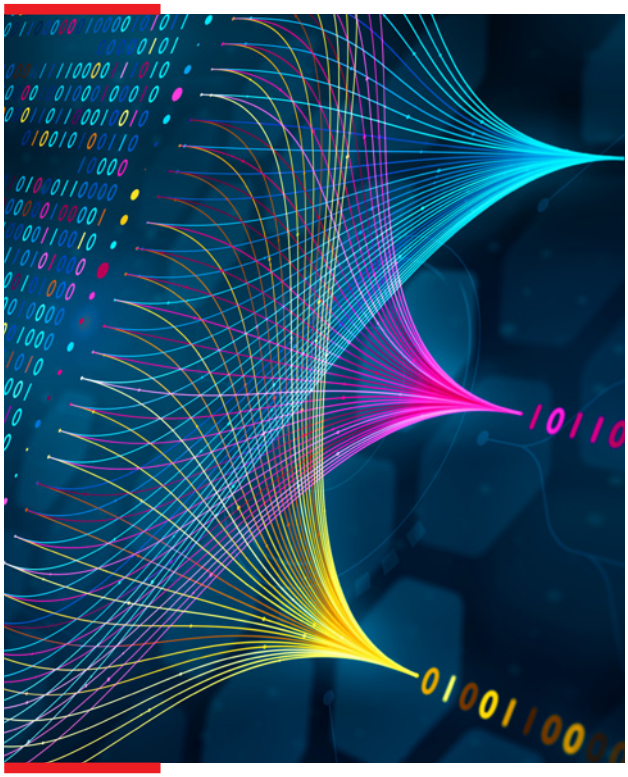
- To ensure EU-wide coherence and cooperation, the AI Act provides for the establishment of the European Artificial Intelligence Board (the **"AI Board"**), comprising representatives from Member States, with specialised subgroups for national regulators and other competent authorities (Article 65).
- The AI Board will play a vital role in ensuring the harmonised implementation of the AI Act. It will serve as the forum where AI regulators, including the AI Office, national authorities and European Data Protection Supervisor (**"EDPS"**), can coordinate the consistent application of the AI Act. The AI Act sets out the AI Board's tasks which include: sharing technical and regulatory expertise and best practices among Member States, and issuing recommendations and written opinions on any matters related to the implementation of the AI Act, and its consistent and effective application (Article 66).

The Advisory Forum

- The Advisory Forum has been established to provide technical expertise and advise the AI Board and the European Commission, and to contribute to their tasks under the AI Act. It will represent a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society and academia. The Advisory Forum will provide stakeholder input by preparing opinions, recommendations and written contributions at the request of the AI Board or the Commission (Article 67).

The Scientific Panel

- The Scientific Panel will advise and support the AI Office, in particular, with implementing and enforcing the AI Act as regards GPAI models and systems; contributing to the development of tools and templates; and supporting the work and activities of market surveillance authorities. The Panel will consist of independent experts selected by the European Commission on the basis of up-to-date scientific or technical expertise in the field of AI (Article 68).



Who is responsible for governance at national level?

National Competent Authorities

- Each Member State must establish or designate as national competent authorities, at least one notifying authority and at least one market surveillance authority to ensure the application and implementation of the AI Act (Article 70).
- A "market surveillance authority" means the national authority designated to carry out the activities and take the measures pursuant to the EU Market Surveillance Regulation (Article 3(26)).
- Member States must communicate to the European Commission the identity of the notifying authorities and the market surveillance authorities, and the tasks of those authorities. Member States must appoint these authorities by **2 August 2025**.
- Whilst Member States generally have discretion to determine which national authorities will operate as market surveillance authorities, the AI Act does prescribe the authority which must serve as a market surveillance authority in respect of certain types of AI systems.
  - For high-risk AI systems related to products covered by the EU harmonisation legislation listed in Section A of Annex I, the market surveillance authority for the purposes of the AI Act shall be the authority responsible for market surveillance activities designated under those legal acts. However, by way of derogation, Member States may designate another relevant authority to act as a market surveillance authority, provided they ensure coordination with the relevant sectoral market surveillance authorities responsible for the enforcement of the EU harmonisation legislation listed in Annex I (Article 74(3)).
  - In addition, for high-risk AI systems placed on the market, put into service, or used by financial institutions regulated by EU financial services law, the market surveillance authority for the purposes of the AI Act shall be the relevant national authority responsible for the financial supervision of those institutions under that legislation in so far as the placing on the market, putting into service, or the use of the AI system is in direct connection with the provision of those financial services. However, again by way of derogation, and provided that coordination is ensured, another relevant authority may be designated as market surveillance authority for the purposes of the AI Act (Articles 74(6) and 74(7)).
  - Furthermore, Member States must designate as the market surveillance authority either the competent data protection supervisory authority under the GDPR or Law Enforcement Directive (2016/680) for high-risk AI systems which fall within the following areas:
    - Annex III(1) (Biometrics), insofar as the systems are used for law enforcement purposes, border management or justice and democracy;
    - Annex III(6) Law Enforcement);
    - Annex III(7) (Migration, Asylum and Border Control Management); and
    - Annex III(8) (Administration of Justice and Democratic Processes) (Article 74(8)).
  - Where EU institutions and bodies or offices fall within the scope of the AI Act, the EDPS will act as market surveillance authority, except in relation to the Court of Justice of the European Union acting in its judicial capacity (Article 74(9)).

11 Post-market Monitoring, Information Sharing and Market Surveillance

In Brief

- Chapter IX, Articles 72-94 set out the rules on post-marketing monitoring, information sharing and market surveillance.
- Providers are required to establish and document a robust "post-market monitoring system" that is proportionate to the nature of the AI technologies and the risks of the high-risk AI system. The post-market monitoring system shall be based on a post-market monitoring plan.
- Providers of high-risk AI systems placed on the EU market must report any "serious incident" to the market surveillance authorities of the Member States where that incident occurred.
- The AI Act brings AI systems within the scope of the EU Market Surveillance Regulation (2019/1020). The effect of this is that operators under the AI Act will be required to comply with the obligations of "economic operators" under the EU Market Surveillance Regulation.
- The AI Act includes a number of provisions that are intended to provide transparency to the bodies involved in the application of the AI Act (such as the European Commission and the market surveillance authorities), these bodies will be required to respect the confidentiality of information and data obtained in carrying out their tasks and activities.

Post-Market Monitoring

- Under the AI Act, a "post-market monitoring system" means all activities carried out by providers of AI systems to collect and review experience gained from the use of AI systems they place on the market or put into service, for the purpose of identifying any need to immediately apply any necessary corrective or preventive action (Article 3(25)).
- Providers are required to establish and document a robust "post-market monitoring system" that is proportionate to the nature of the AI technologies and the risks of the high-risk AI system (Article 72(1)).
- The post-market monitoring system must actively collect, document and analyse relevant data, which may be provided by deployers or collected through other sources, on the performance of high-risk AI systems throughout their lifetime. The data collected must allow the provider to evaluate the continuous compliance of their high-risk AI system with the requirements set out in Section 2 of Chapter III (Articles 8-15) (Article 72(2)).
- A provider should ensure its contracts with deployers and/or other relevant third parties, includes a provision to require the deployer to provide information about the performance of the AI system to help the provider evaluate its compliance with the requirements in Section 2 of Chapter III.
- The post-market monitoring system shall be based on a post-market monitoring plan. That plan, in turn, shall be part of the technical documentation referred to in Annex IV, which the provider must retain. The European Commission has an obligation to establish a template for the post-market monitoring plan by **2 February 2026** (Article 72(3)).

Reporting of Serious Incidents

- Providers of high-risk AI systems placed on the EU market must report any serious incident to the market surveillance authorities of the Member States where that incident occurred (Article 73(1).
- A "serious incident" means an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:

  (a) The death of a person, or serious harm to a person's health.

  (b) A serious and irreversible disruption of the management or operation of critical infrastructure.

  (c) The infringement of obligations under EU law intended to protect fundamental right.

  (d) Serious harm to property or the environment (Article 3(49)).
- A serious incident must be reported within the following time-frames:
  - immediately after the provider has established a causal link between the AI system and the serious incident or the reasonable likelihood of such a link, and in any event, not later than **15 days** after the provider or, where applicable, the deployer, becomes aware of the serious incident; or

- immediately but not later than **10 days** in respect of a serious incident involving a person's death; or
- immediately but not later than **two days** in respect of a serious and irreversible disruption of the management or operation of critical infrastructure or a "widespread infringement" as defined in Article 3(61) (i.e. an act or omission contrary to EU law which is likely to arm the collective interests of individuals residing in multiple Member States) (Article 73(2)-(4)).

- Where necessary, to ensure timely reporting, the provider, or the deployer (where applicable), may submit an initial report that is incomplete, followed by a complete report (Article 73(5)).
- Action to be taken by a provider following the reporting of a serious incident:
  - The provider must, without undue delay, conduct an investigation into the serious incident and the AI system concerned, and perform a risk assessment of the incident and take any necessary corrective action.
  - The provider must cooperate with the competent authorities, and not perform any investigation which involves altering the relevant AI system in a way that may affect any evaluation of the causes of the incident, prior to informing the competent authorities of such action (Article 73(6)).
- The European Commission is obliged to develop guidance to facilitate compliance with the serious incident reporting obligations by **2 August 2025**, and keep that guidance under review (Article 73(7)).
- Articles 73(9)-(10) contains certain limitations to the reporting obligation, as follows:
  - For high-risk AI systems referred to in Annex III, that are placed on the EU market or put into service by providers that are subject to EU legislative instruments laying down reporting obligations equivalent to those set out in the AI Act, the notification of serious incidents shall be limited to those referred to in Article 3(49)(c) of the AI Act.
  - In addition, for high-risk AI systems which are safety components of devices, or devices themselves, covered by Medical Device Regulations (EU) 2017/745 and (EU) 2017/746, the notification of serious incidents shall be limited to those referred to in Article 3(49)(c) of the AI Act, and shall be made to the national competent authority chosen for that purpose by the Member State where the incident occurred.
- Market Surveillance authorities must take appropriate measures, as provided for in Article 19 of the EU Market Surveillance Regulation, within seven days of receipt of a serious incident notification, and must follow the notification procedures provided in that Regulation. National competent authorities must immediately notify the European Commission of any serious incident, whether or not they have taken action on it, in accordance with Article 20 of the EU Market Surveillance Regulation (Article 73(8) and (11)).

Market Surveillance and Control of AI systems in the EU market

- The AI Act brings AI systems within the scope of the EU Market Surveillance Regulation. The effect of this is that operators under the AI Act will be required to comply with the obligations of "economic operators" under the EU Market Surveillance Regulation (Article 74(1)).
- Market surveillance authorities have broad enforcement powers under the EU Market Surveillance Regulation and the AI Act to require providers to grant full access to information and documentation about AI systems, including the training, validation and testing data sets used for the development of high-risk AI systems; conduct investigations, and evaluate compliance with the AI Act (Article 74(11)-(12)).
- Market surveillance authorities can also request access to the source code of a high-risk AI system, subject to statutory confidential obligations, where the following conditions apply:
  - Access to the source code is necessary to assess the conformity of a high-risk system with the technical requirements set out in Chapter III, Section 2, Articles 8-15; and
  - Testing or auditing procedures and verifications based on the data and documentation provided by the provider have been exhausted or proved insufficient (Article 74(13)).
- Market Surveillance authorities can require operators to take certain corrective actions if they find that any high-risk AI systems "present a risk" (as defined in Article 3(19) of the EU Market Surveillance Regulation), insofar

as they present risks to health or safety, fundamental rights, of persons, and are not in compliance with the AI Act. Where the operator of an AI system does not take adequate corrective action within the specified period, then market surveillance authorities may prohibit or restrict the system from being made available on its national market or put into service, or withdraw or recall it (Article 79(1)-(5)).

- Market surveillance authorities may require a provider to put an end to any of the following acts of non-compliance, within a specified period:
  - CE marking has been affixed in violation of Article 48.
  - CE marking has not been affixed.
  - EU declaration of conformity referred to in Article 47 has not been drawn up.
  - EU declaration of conformity referred to in Article 47 has not been drawn up correctly.
  - Registration in the EU database referred to in Article 71 has not been carried out;
  - No authorised representative has been appointed (where applicable).
  - Technical documentation is not available (Article 83).
- If the provider fails to take appropriate corrective action in regard to the above acts, then the market surveillance authority concerned may restrict or prohibit the high-risk AI system from being made available on the EU market, or ensure it is recalled or withdrawn without delay.

Confidentiality

- The AI Act includes a number of provisions that are intended to provide transparency to the bodies involved in the application of the AI Act (such as the European Commission and the market surveillance authorities), these bodies will be required to respect the confidentiality of information and data obtained in carrying out their tasks and activities (Article 78(1)).
- The confidentiality requirement applies, for example, to any information and documentation provided by providers of high-risk AI systems to national competent authorities to demonstrate conformity of their high-risk AI systems with the requirements of Chapter II (pursuant to Article 21) and any information and documentation (including trade secrets) made available by providers of GPAI models or GPAI models with systemic risk, including documentation about the purpose, training and testing of the models (pursuant to Articles 53 and 55).
- The bodies involved in the application of the AI Act (including the European Commission, market surveillance authorities, notified bodies, and any other natural or legal person) must:
  - only request data that is strictly necessary to carry out their compliance responsibilities;
  - put in place adequate cybersecurity measures to protect security and confidentiality of such information and data; and
  - delete the data collected as soon as it is no longer needed for the purpose for which it was obtained (Article 78(2)).
- Before sharing information on certain high-risk AI systems used by law enforcement border control, immigration or asylum authorities with other national competent authorities or the European Commission, national competent authorities must first consult with the provider if such sharing could jeopardize public and national security interests. In addition, where such law enforcement border control, immigration or asylum authorities are the providers of such high-risk AI systems, only staff of the market surveillance authority with the appropriate level of security clearance may access the

relevant technical documentation at the premises of such authorities (Article 78(3)). These restrictions are without prejudice to the exchange of information and the dissemination of warnings, between the European Commission, the Member States and their relevant bodies, and to the obligations of these parties to provide information under the criminal law of the Member States (Article 78(4)).

- Notwithstanding the above, the European Commission and Member States may exchange confidential information with regulatory authorities of third countries, provided that such exchange is necessary and in accordance with relevant provisions of international and trade agreements (Article 78(5)).

Right to lodge a complaint with a market surveillance authority

- Article 85 permits any natural or legal person who considers there has been an infringement of the AI Act to submit complaints to the relevant market surveillance authority.

Right to explanation of individual decision-making

- Deployers must provide clear and meaningful explanations for decisions taken on the basis of the output from a high-risk AI systems listed in Annex III (with the exception of systems listed under Annex III(2)), which produces legal effects or similarly significantly affects that person in a way which any individual considers adversely impacts their health, safety and fundamental rights (Article 86(1)).
- This provision only applies to the extent that this right is not otherwise provided for under EU law, and should accordingly not apply in circumstances where the person is already entitled to this information under Article 22 GDPR (Article 86(3)).

12 Enforcement and Penalties

In Brief

- Articles 99-101 set out the rules in respect of penalties to be imposed following non-compliance with the AI Act.
- The fines range from €7.5 million or 1% of an undertaking's global annual turnover to €35 million or 7% of an undertaking's global annual turnover, depending on the nature of the infringement.
- The potential for regulatory sanctions and reputational damage serve as strong deterrents for businesses to avoid breaching their obligations under the AI Act.

Timeline for implementation of AI Act and issuing of fines

- Article 99, which sets out the fines that may be imposed by Member States for non-compliance with the AI Act, including non-compliance with the rules on prohibited practices referred to in Article 5, comes into force on **2 August 2025**. However, the ban on prohibited AI practices itself comes into effect on **2 February 2025**. This means that enforcement of the ban on prohibited AI practices may be left to private litigation for the first six months.
- In addition, it is worth noting that although requirements for providers of GPAI models become applicable on **2 August 2025**, the related fines (which can be imposed by the European Commission pursuant to Article 101) in principle only start applying 12 months later, on **2 August 2026** (see *Timeline to Implementation*).

Fines for infringements of the AI Act

- Member States are required to lay down "effective, proportionate and dissuasive" penalties for infringements of the rules for AI systems, and notify the European Commission of those rules. However, Article 99(1) sets out specific maximum thresholds which apply in respect of infringement of the following obligations:

▪ **Prohibited Practices (Article 5)**	Up to €35m or, if the offender is an undertaking, up to 7% of the total global annual turnover (whichever is higher)
▪ **High-risk AI system obligations of Providers (Article 16)** ▪ **High-risk AI system obligations of Authorised Representatives (Article 22)** ▪ **High-risk AI system obligations of Importers (Article 23)** ▪ **High-risk AI system obligations of Distributors (Article 24)** ▪ **High-risk AI system obligations of Deployers (Article 26)** ▪ **Requirements and obligations of Notified Bodies (Articles 31, 33(1), 33(3) and 33(4) or 34)** • **Transparency Obligations (Article 50)**	Up to €15m or, if the offender is an undertaking, up to 3% of the total global annual turnover (whichever is higher)
▪ **Supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request**	Up to €7.5m or, if the offender is an undertaking, up to 1% of the total global annual turnover (whichever is higher)

- For each category of infringement, the threshold will be the lower of the two amounts for SMEs, including start-ups, and the higher for other companies (Article 99(6)). This leniency does not, however, appear to have been expressly extended to fines for providers of GPAI models (see *Fines for Providers of GPAI Models*).
- The penalties set out in Article 99(1) include a reference to the turnover of the "undertaking". This suggests that fines are intended to be calculated based on the turnover of the group, rather than just the individual entity responsible for non-compliance, in a manner similar to the GDPR. However, the AI Act lacks any wording explicitly confirming this approach. In particular, the recitals do not contain any wording similar to that contained in Recital 150 of the GDPR, which states that "where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes". Accordingly, guidance from the European Commission will be welcomed on this issue.

- Member States have been provided with discretion to lay down the rules on the extent to which administrative fines may be imposed on public authorities and bodies (Article 99(8)).
- The AI Act also leaves it to Member States to determine whether the fines are imposed by competent national courts or by other bodies (Article 99(9)).
- When determining whether to impose an administrative fine, and the amount of that fine, Article 99(7) sets out a list of factors that must be taken into account.

Fines for Providers of GPAI Models

- Article 101(1) enables the European Commission (and AI Office) to enforce the rules on providers of GPAI models by means of fines, where it finds that the provider has intentionally or negligently committed any of the following infringements:

▪ **Infringed the relevant provisions of the AI Act** ▪ **Failed to comply with a request by the European Commission for a document or for information pursuant to Article 91, or supplied incorrect, incomplete or misleading information** ▪ **Failed to comply with a measure requested by the European Commission under Article 93** ▪ **Failed to make available to the European Commission access to the GPAI model or GPAI model with systemic risk with a view to conducting an evaluation pursuant to Article 92**	Up to €15m or 3% of the total worldwide annual turnover (whichever is higher)

- In fixing the amount of the fine or periodic penalty payment, the European Commission will have regard to the nature, gravity and duration of the infringement, taking due account of the principles of proportionality and appropriateness. The Commission shall also into account commitments made in accordance with Article 93(3) or made in relevant codes of practice in accordance with Article 56. Any fine imposed must be "effective, proportionate, and dissuasive" (Articles 101((1) and (3)).
- Before adopting a decision on a fine, the European Commission will communicate its preliminary findings to the provider of the GPAI model, and provide it with an opportunity to be heard (Article 101(2)).
- The EU Court of Justice will have unlimited jurisdiction to review decisions of the European Commission in regard to fines, and may cancel, reduce or increase the fine imposed (Article 101(5)).

13 AI Regulatory Sandboxes

In Brief

- Chapter VI (Articles 57-63) sets out a framework for promoting AI innovation, in particular through AI regulatory sandboxes.
- National authorities must establish at least one AI regulatory sandbox at national level, which will be operational by 2 August 2026 (Article 57(1)).

What are AI Regulatory Sandboxes?

- An AI regulatory sandbox is defined as a controlled framework set up by a competent authority to offer 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 (Article 3(55)).
- A sandbox plan, in turn, means a document agreed between the participating provider and the competent authority describing the objectives, conditions, timeframe, methodology, and requirements for the activities carried out within the sandbox (Article 3(54)).
- AI regulatory sandboxes aim to enhance legal certainty for innovators and the competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI use, to facilitate regulatory learning for authorities and undertakings, including with a view to future adaptions of the legal framework (Recital 139).

Role of National Authorities

- National authorities must establish at least one AI regulatory sandbox at national level, which must be operational by 2 August 2026 (Article 57(1)).
- National authorities are tasked with providing guidance, supervision and support throughout the sandbox lifecycle, identifying risks, in particular to fundamental rights, health and safety (Article 57(6)).
- National authorities must issue exit reports, detailing the activities carried out in the sandbox and the related results and learning outcomes. Providers may use such documentation to demonstrate their compliance with the AI Act. The European Commission and the AI Board have authority to access the exit reports and take them into account when exercising their regulatory tasks under the AI Act (Article 57(7)-(8)).
- National competent authorities have the power to temporarily or permanently suspend sandbox activities, if no effective mitigation is possible, and must inform the AI Office of such a decision (Article 57(11)).
- National authorities must also collaborate to maintain consistent practices across the EU by submitting annual reports to the AI Office and the AI Board on sandbox implementation (Article 57(16)).

Personal Data

- National authorities must ensure that, to the extent the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of national data protection authorities (**"DPAs"**), that those DPAs are associated with the operation of the AI regulatory sandbox and involved in the supervision of those aspects to the extent of their respective tasks and powers (Article 57(10)).
- The processing of personal data in AI regulatory sandboxes must comply with EU and applicable national laws.
- Personal data lawfully collected for other purposes may be processed for the purpose of developing, training, and testing certain AI systems in the sandbox, subject to a number of specified conditions set out in Article 59(1)(a)-(j) being met. In particular, the AI system must be developed for safeguarding substantial public interests by a public authority or other natural or legal person in one or more of the following areas:
  - Public safety and public health, including disease detection, diagnosis prevention, control, treatment and improvement of health care systems.
  - A high level of protection and improvement of the quality of the environment, protection of biodiversity, protection against pollution, green transition measures, climate change mitigation, and adaptation measures.
  - Energy sustainability.
  - Safety and resilience of transport systems and mobility, critical infrastructure, and networks.
  - Efficiency and quality of public administration and public services.

Providers' Liability for Sandbox Activities

- The innovation support measures set out in Chapter VI reflect a modern legal landscape. Providers and prospective providers participating in the AI regulatory sandbox remain liable for any damage inflicted on third parties during sandbox activities. However, provided that the prospective providers observe the specific plan and the terms and conditions for their participation and follow in good faith the national guidance, then no administrative fines will be imposed by national authorities for infringements of the AI Act (Article 57(12)).

Role of EU Commission and AI Office

- To avoid fragmentation across the EU, the European Commission will adopt implementing acts clarifying sandbox modalities, development, and operations, including eligibility criteria, application procedures, and participant terms. At EU level, the European Commission will also adopt a unified interface to facilitate interaction among Member States and stakeholders (Article 58).
- The AI Office shall make publicly available a list of planned and existing sandboxes and keep it up-to-date in order to encourage more interaction in the AI regulatory sandboxes and cross-border cooperation (Article 57(15)).

Testing in Real-World Conditions

- Providers or prospective providers of high-risk AI systems listed in Annex III may test them in real-world conditions, outside AI regulatory sandboxes, if they respect certain conditions set out in Article 60(4) of the AI Act, including drawing up a real-world testing plan and submitting it to the relevant market surveillance authority, and obtaining informed consent from the subjects of the real-world testing.
- The provider or prospective provider will, however, be liable under applicable EU and national liability law for any damage caused in the course of their testing in real world conditions (Article 60(9)).

Matheson

14 Timeline to implementation

In Brief

- The AI Act introduces a complicated matrix of deadlines and transitional periods that are fast approaching.

12 July 2024

The AI Act is published in the Official Journal of the European Union.

1 August 2024

The AI Act comes into force *(Art. 113)*.

2 February 2025

Rules on prohibited AI systems, scope, definitions and AI literacy come into force *(Art. 113(a))*.

2 May 2025

AI Office Codes of Practice must be made available for providers of General Purpose AI ("**GPAI**") models *(Art. 56(9))*.

2 August 2025

Rules on notifications, governance and certain penalties come into force. Also, rules applicable to GPAI models placed on the EU market on or after 2 August 2025 come into force *(Art. 113(b))*. However, providers of GPAI models that are placed on the EU market prior to 2 August 2025, have an additional two years to comply, until 2 August 2027 *(Art. 111(3))*.

2 February 2026

EU Commission must provide guidelines specifying the practical implementation of the AI Act, together with a comprehensive list of practical examples of use cases of AI systems that are high-risk and not high-risk *(Art. 6(5))*.

2 August 2026

The AI Act is generally applicable, including for high-risk AI systems under Art. 6(2) (as set out in Annex III), which are placed on the EU market, or are significantly changed, on or after 2 August 2026 *(Art. 113))*. However, operators of high-risk AI systems that are placed on the EU market prior to 2 August 2026, and are not intended for use by public authorities, only need to comply with the AI Act in the event of a significant design change (with the exception of compliance with the rules on prohibited AI systems under Art. 5, which must not be used from 2 February 2025) *(Art. 111(2))*.

2 August 2027

Provisions applicable to high-risk systems designed to be used as part of safety components in regulated products under Art. 6(1), and are placed on the EU market on or after 2 August 2026, come into effect *(Art. 113(c))*.

2 August 2030

Operators of high-risk AI systems that are placed on the EU market before 2 August 2026, and are intended for use by public authorities, must comply with the AI Act by 2 August 2030, regardless of whether there has been a significant design change or not *(Art. 111(2))*.

31 December 2030

Operators of AI systems that are components of large-scale IT systems established by legal acts listed in Annex X, and that have been placed on the EU market before 2 August 2027, have until 31 December 2030 to comply with the AI Act. However, the rules on prohibited AI systems under Art. 5 still apply, and must not be used from 2 February 2025 *(Art. 111(1))*.

15 Forthcoming Guidance, Codes of practice, Implementing and Delegated Acts

In Brief

- The AI Act is a lengthy and complex EU Regulation, and is accordingly due to be supplemented by guidelines, templates, and codes of practice and implementing acts at EU level.
- It also empowers the European Commission to adopt delegated acts in order to take account of evolving technological developments future-proof the Act.

Guidelines

- Article 96 requires the European Commission to develop guidelines on the practical implementation of the AI Act, to help organisations understand their obligations and promote compliance. These guidelines will cover, in particular:
  - The technical requirements of providers of high-risk systems and responsibilities along the AI value chain (as set out in Articles 8-15 and Article 25).
  - Prohibited AI practices referred to in Article 5.
  - The practical implementation of the provisions relating to "substantial modification".
  - The practical implementation of transparency obligations laid down in Article 50.
  - 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.
  - The application of the definition of an AI system, as set out in Article 3(1).

Templates and Voluntary Model Contract Terms

- The European Commission will also publish templates to help organisations comply with their new obligations under the AI Act, including, for example: (i) a template post-market monitoring plan (Article 72); (ii) a template to assist providers with completing a summary of the content used for training GPAI models (Article 53); and (iii) a template questionnaire to assist deployers with complying with their obligations regarding a FRIA (Article 27).
- In addition, the Commission, through its AI Office, may develop and recommend voluntary model terms for contracts between providers of high-risk AI systems and third parties that supply tools, services, components, or processes that are used for or integrated into high-risk AI systems (Article 25(4)).

Codes of Practice and Implementing Acts

- The AI Office is required to facilitate the drawing up of codes of practice at EU level in order to contribute to the proper application of the AI Act, taking into account international approaches (Article 56).
- In particular, the AI Office is expected to draw up a code of practice to facilitate the effective implementation of the transparency obligations of providers and deployers regarding the detection and labelling of artificially generated or manipulated content. If it deems the code of practice to be inadequate, the Commission may adopt an implementing act specifying common rules for the implementation of these obligations (Article 50).
- The AI Office is also required to ensure that the codes of practice cover the obligations of providers of GPAI models. Such providers will be able to rely on codes of practice to demonstrate compliance with their obligations, until a harmonised standard is published (Article 53(4)). Obligations for providers of GPAI models apply from 2 August 2025, and codes of practice are due to be published by 2 May 2025, in order to enable providers to demonstrate compliance on time (Recital 179 and Article 56). In the event that a code of practice cannot be finalised by 2 August 2025, or if the AI Office deems it inadequate following its assessment, the Commission may provide, by means of implementing acts, common rules for the implementation of the obligations of providers of GPAI models (Article 56).
- The European Commission may also adopt implementing acts specifying detailed arrangements for the establishment, development, implementation, operation and supervision of AI regulatory sandboxes, and the real-world testing plan (Articles 58 and 60).
- The European Commission may also adopt implementing acts to detail arrangements and procedural safeguards for proceedings aimed at imposing fines in respect of providers of GPAI models (Article 101).

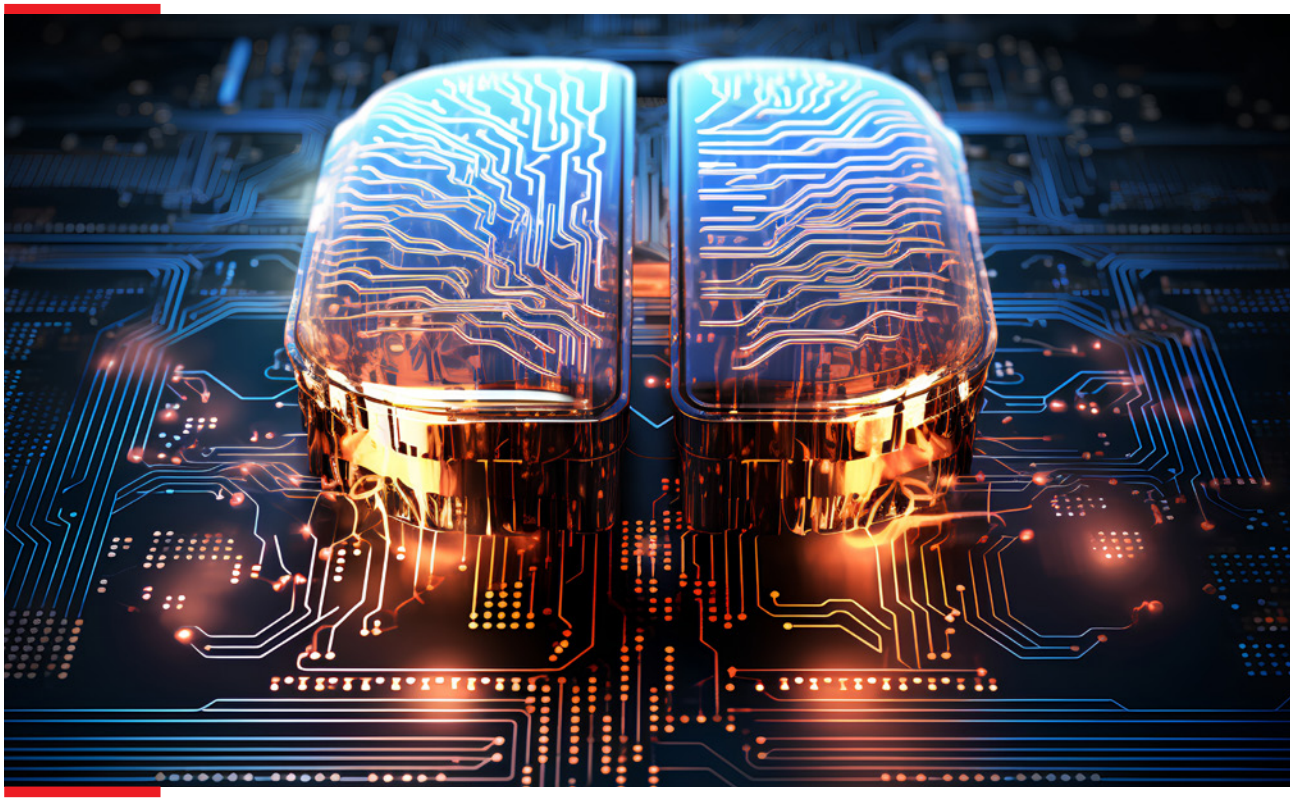
Delegated Acts

- The European Commission is empowered to adopt a number of delegated acts in accordance with Article

97. These delegated acts empower the Commission, in particular, to:

- Amend the conditions laid down in Article 6(3) (which sets out four conditions when an AI system referred to in Annex II shall not be considered high-risk, as it poses no significant risk of harm), by adding new conditions or modifying them, where there is evidence of the existence of AI systems that fall under the scope of Annex III, but do not pose a significant risk of harm to the health, safety or fundamental rights of individuals (Article 6(6)).
- Amend the conditions laid down in Article 6(3), by deleting any of the conditions laid down therein, where there is evidence that this is necessary to maintain the level of protection of health, safety and fundamental rights provided for by the AI Act (Article 6(7)).
- Amend Annex III by adding or modifying high-risk AI systems where specified conditions are fulfilled (Article 7(1)).
- Amend the list in Annex III by removing high-risk AI systems where specified conditions are fulfilled (Article 7(3)).
- Amend Annex IV (which lists the information to be included in technical documentation drawn up by providers of high-risk AI systems), to ensure, in light of technical progress, the documentation provides all the information necessary to assess the compliance of the AI system with the requirements set out in Section 2 of Chapter III (Article 11(3)).
- Amend Annexes VI and VII (which concern, respectively, the self-assessment conformity process, and conformity assessment process by a notified body) by updating them in light of technical progress (Article 43(5)).
- Amend Article 43(1) and (2) in order to subject high-risk AI systems referred to in Annex III (2)-(8) to the conformity assessment process by a notified body (rather than to the self-assessment conformity process), as set out in Annex VII or parts thereof (Article 43(6)).
- Amend Annex V by updating the content of the EU declaration of conformity set out in that Annex, in order to include other information that becomes necessary in light of technical progress (Article 47(5)).
- Amend the thresholds listed in Article 51(1) and (2) (which set out when a GPAI model should be classified as a GPAI model with systemic risk), as well as 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 51(3)).
- Amend Annex XIII (concerning the criteria for designation of a GPAI model with systemic risk), by specifying and updating the criteria set out in this Annex (Article 52(4)).
- For the purpose of facilitating compliance with Annex XI (concerning technical documentation and information to be provided by providers of all GPAI models), in particular concerning the computational resources used to train the GPAI model (such as number of floating point operations), the Commission may detail measurement and calculation methodologies with a view to allowing for comparable and verifiable documentation (Article 53(5)).
- Amend Annexes XI and XII (concerning, respectively, technical documentation and transparency information to be provided by providers of GPAI models), in light of evolving technological developments (Article 53(6)).

16 How to prepare for the AI Act?



Companies should consider taking the following steps in preparation for the implementation of the AI Act:

- **Map your development and/or use of AI systems.** Identify all AI systems your company is developing or using or planning to use. Consider the intended purpose and function of the systems, and the data processed.
- **Classify your AI systems or GPAI model.** Determine whether your company's AI system falls within the prohibited, high-risk, limited risk, or minimal risk categories, or whether it is a GPAI model with or without systemic risk. Consider, in particular, whether the system involves customer interaction, generates content which may pose specific risks of impersonation or deception, or makes automated decisions which have a high potential to cause significant harm to the health, safety or fundamental rights of individuals.
- **Assess which operator role your company is playing.** Consider, in particular, whether your company is a provider or deployer of a high-risk AI system or a provider of a GPAI model with or without systemic risk.
- **Appoint an AI governance working group to steer AI compliance efforts.** Establish internal rules for the usage and approval of AI solutions.
- **Develop a compliance strategy and assign sufficient resources for compliance.** Discontinue or modify non-compliant AI systems. Establish AI policies and procedures for ongoing monitoring and assessment of your company's compliance with the AI Act.
- **Educate employees on AI policies.** Provide employees with written guidelines and other materials, including educational training sessions on your company's obligations under the AI Act. Ensure they have the skills and knowledge, taking into account your company's rights and obligations, to make an informed deployment of AI systems, and to identify and mitigate risks of AI and possible harm that it can cause.
- **Keep up-to-date records of your use of AI systems or models, risk assessments, and compliance measures.** Ensure you can demonstrate your compliance to regulatory authorities on request, and provide any necessary documentation.

Key contacts

Anne-Marie Bohan
Partner
T +353 1 232 2212
E anne-marie.bohan@matheson.com

Davinia Brennan*
Partner
T +353 1 232 2700
E davinia.brennan@matheson.com

Deirdre Crowley
Partner
T +353 21 465 8219
E deirdre.crowley@matheson.com

Sarah Jayne Hanna
Partner
T +353 1 232 2865
E sarahjayne.hanna@matheson.com

Carlo Salizzo
Partner
T +353 1 232 2011
E carlo.salizzo@matheson.com

Alice Duffy
Partner
T +353 1 232 2053
E alice.duffy@matheson.com

*Acknowledgements

With special thanks to Davinia Brennan, Partner, Technology & Innovation Group, for her significant work on this Guide.

Matheson

DUBLIN
70 Sir John Rogerson's Quay,
Dublin 2
Ireland

T: +353 1 232 2000
E: dublin@matheson.com

CORK
Penrose One,
Penrose Dock,
Cork, T23KW81

T: +353 21 465 8200
E: cork@matheson.com

LONDON
Octagon Point,
5 Cheapside,
London EC2V 6AA

T: +44 20 7614 5670
E: london@matheson.com

NEW YORK
200 Park Avenue
New York, NY 10166
United States

T: +1 646 354 6582
E: newyork@matheson.com

PALO ALTO
530 Lytton Avenue
Palo Alto, CA 94301
United States

T: +1 650 617 3351
E: paloalto@matheson.com

SAN FRANCISCO
156 2nd Street
San Francisco CA 94105
United States

T: +1 650 617 3351
E: sf@matheson.com